Universidad Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

Modelo de Privacidad Digital en Inteligencia Ambiental basado en Sistemas Multiagente

Autor:

Mª del Mar López Ruiz

Director/es:

José Manuel Molina López

Javier Carbó Rubiera

Tutor:

José Manuel Molina López

DEPARTAMENTO DE INFORMÁTICA

Leganés, Mayo de 2017

Universidad Carlos III de Madrid
www.uc3m.es

TESIS DOCTORAL

Modelo de Privacidad Digital en Inteligencia Ambiental basado en Sistemas Multiagente

Autor: Mª del Mar López Ruiz

Director/es: José Manuel Molina López

Javier Carbó Rubiera

Firma del Tribunal Calificador:

Firma

Presidente: (Nombre y apellidos)

Vocal: (Nombre y apellidos)

Secretario: (Nombre y apellidos)

Calificación:

Leganés, de de

“A Silvia, Álex y Paco”

"Cada nuevo amigo que ganamos en la carrera de la vida
nos perfecciona y enriquece más aún
por lo que de nosotros mismos nos descubre,
que por lo que de él mismo nos da"

(Miguel de Unamuno)

"Confía en el tiempo, que suele dar dulces salidas a
muchas amargas dificultades"

(Miguel de Cervantes Saavedra)

"La vida sólo puede ser comprendida hacia atrás,
pero únicamente puede ser vivida hacia delante"

(Sören Kierkegaard)

"Agradecimientos"

La realización de esta tesis me ha dado la oportunidad de embarcarme en una gran aventura de aprendizaje tanto académico como personal, por lo que debo dar las gracias a todas las personas que me han acompañado en este viaje.

Quiero dar las gracias a mis directores de tesis, los profesores José Manuel Molina y Javier Carbó por haber confiado en mí, por su paciencia para guiar mis pasos de manera tan acertada, y por el tiempo que han dedicado a resolver mis innumerables dudas.

Gracias también a los profesores Antonio Berlanga, Jesús García, Miguel Ángel Patricio, Juanita Pedraza y Sergio Velastín por su total predisposición para ayudarme en las diferentes tareas realizadas desde que inicie esta nueva etapa profesional en la Universidad Carlos III de Madrid. También quiero agredecer la excelente relación que he tenido con todos los miembros del Grupo GIAA de la UC3M; gracias especialmente a Álvaro Luis, Enrique Martí, José Luis Guerrero, Gonzalo Blázquez, Juan Gómez, Nayat Sánchez y Luis Martí.

También quiero agradecer todo el apoyo y cariño de mi gran familia, gracias Mercedes. Y gracias a todos los amigos con los que he tenido la suerte de compartir tantos momentos, gracias de todo corazón.

Y sobre todo, muchas gracias a las tres personas que han sido mi mochila en esta aventura; GRACIAS a Paco, Álex y Silvia, sois lo mejor que me ha dado la vida.

No quiero terminar sin dedicar un emotivo recuerdo a mi cuñado Gregorio por haberme embarcado en este gran viaje. Gracias.

M. Mar López
Colmenarejo, Mayo de 2017

Resumen

El gran desarrollo de las Tecnologías de la Información y la Comunicación utilizadas en los dominios de aplicación de la Inteligencia Ambiental (AmI), ocurrido en la última década, nos sitúa inmersos en los llamados entornos inteligentes, rodeados de una extensa variedad de dispositivos y tecnologías con capacidad de adquirir, almacenar y transmitir nuestra información personal. La complejidad y volumen de los sistemas involucrados en las aplicaciones desarrolladas en Inteligencia Ambiental hacen que seamos incapaces de conocer y controlar toda la información que estos sistemas son capaces de adquirir y transmitir, tanto si esta información ha sido proporcionada por nosotros directamente, como si ha sido adquirida de forma indirecta por otros sistemas sin nuestro conocimiento; lo que pone en riesgo la protección de nuestro derecho a la privacidad.

Considerando que, el principal objetivo de la Inteligencia Ambiental es el de ofrecernos diferentes tipos de servicios personalizados en cualquier lugar y en todo momento, facilitándonos así la realización de nuestras actividades cotidianas, se ha llevado a cabo un estudio sobre las aplicaciones desarrolladas en AmI, que ha revelado la necesidad de incluir las cuestiones de tipo social y ético en el diseño del AmI, destacando entre ellas la privacidad por ser uno de los derechos fundamentales de las personas, como así queda reflejado en la Declaración Universal de los Derechos Humanos (Artículo 12).

Por ello, para el verdadero desarrollo y aceptación de la Inteligencia Ambiental deberá considerarse no solo los aspectos tecnológicos, sino que, resulta fundamental tener en cuenta las implicaciones sociales y éticas. Esta es la idea del concepto “Design by Privacy” que se ha utilizado en la investigación realizada. En base a este concepto, se han establecido las políticas de privacidad del usuario según los dominios de aplicación del AmI.

Partiendo de la base de que sean las propias técnicas utilizadas en AmI las que ayuden a proteger nuestra información personal, se han utilizado los agentes de los modelos de confianza como herramienta para determinar los derechos de privacidad que deben cumplir los agentes en sus comunicaciones, y que ha servido para decidir con quién compartimos nuestras opiniones privadas, minimizando de esta forma los riesgos de la privacidad de nuestra información al interaccionar con los servicios ofrecidos por las aplicaciones del AmI.

Así pues, el motivo de investigación de esta tesis es el de presentar un Modelo de Privacidad Digital basado en Sistemas Multiagente, que nos ayudará a decidir en quién confiar a la hora de compartir nuestras opiniones privadas. Este modelo ha sido implementado para su validación en el entorno de experimentación del ART testbed (Agent Reputation and Trust), en el que el dominio de aplicación del AmI es el relacionado con la tasación de cuadros o pinturas de arte. Una vez implementada la manera de decidir con quién compartimos nuestra información privada, y con el fin de controlar el cumplimiento de los derechos de privacidad que se han establecido en las comunicaciones entre los agentes, se han formalizado las posibles infracciones sobre los derechos de privacidad utilizando la Institución Electrónica "Islander" como herramienta de especificación de las normas y sanciones correspondientes que deben cumplir los agentes en sus comunicaciones.

Palabras Clave: Inteligencia Ambiental, Entornos Inteligentes, Privacidad, Confianza, Dominio del usuario, "Design by Privacy", Políticas de privacidad, Derechos de privacidad, Modelos de Confianza, Agentes Inteligentes, Sistemas Multiagente, Instituciones Electrónicas.

Abstract

The great development of Information and Communication Technologies used in the domains of application of Ambient Intelligence, which has taken place in the last decade, places us immersed in intelligent environments surrounded by a wide variety of devices and Technologies with the ability to acquire, store and transmit our personal information. The complexity and volume of the systems involved in the applications developed in Environmental Intelligence mean that we are unable to know and control all the information that these systems are able to acquire and transmit, whether this information has been provided by us directly, or whether it has Been acquired indirectly by other systems without our knowledge; Which puts at risk the protection of our right to privacy.

Considering that the main objective of Environmental Intelligence is to offer different types of personalized services in any place and at all times, facilitating us to carry out our daily activities, a study has been carried out on the applications developed in AmI, which has revealed the need to take into account social and ethical issues in the design of the AmI, highlighting among them the privacy as one of the fundamental rights of the people, as reflected in the Universal Declaration of Human Rights (Article 12).

For that reason, for the true development and acceptance of Ambient Intelligence, not only the technological aspects must be taken into account, but it is fundamental to consider the social and ethical implications. This is the idea of the concept "Design by Privacy" that has been used on the research carried out. Based on this concept, user privacy policies have been established and should be taken into account in the AmI application domains.

Based on the idea that the techniques used in AmI are those that help protect our personal information, the agents with a trust model have been used as a tool to determine the privacy rights that agents must comply with in their communications, and that has served to decide with whom we share our private opinions, thus minimizing the risks of privacy of our information when interacting with the services offered by AmI applications.

Therefore, the aim of the research of this thesis is to present a Digital Privacy Model based on Multi-Agent Systems, which will help us to decide who to trust when sharing our private opinions. This model has been implemented for validation in the experimental environment of the ART testbed (Agent Reputation and Trust), in which the domain of the AmI application, is the one related with the evaluation of art pictures. Once the way to decide with whom we share our private information has been implemented, and in order to control the compliance with the privacy rights established in the communications between the agents, possible violations of privacy rights have been formalized using the Electronic Institution "Islander" as a tool for specifying the standards and corresponding sanctions that agents must comply with in their communications.

Keywords: Ambient Intelligence, Intelligent Environments, Privacy, Trust, User´s domain, Design by Privacy, Privacy Policies, Rights to Privacy, Trust Models, Intelligent Agents, Multiagent Systems, Electronic Institutions.

PARTE I. INTRODUCCIÓN

PARTE II. ESTADO DEL ARTE

PARTE I

INTRODUCCIÓN

Capítulo 1

Introducción

1.1. INTRODUCCIÓN

La Inteligencia Ambiental (AmI) constituye una evolución de las Tecnologías de la Información y la Comunicación (TICs) que responde a la demanda actual de disponer de diferentes tipos de servicios y de información, en cualquier lugar, y en todo momento. La Inteligencia Ambiental engloba una amplia variedad de tecnologías con capacidad sensorial, gran poder de procesamiento, y mecanismos de razonamiento que facilitan la comunicación entre diferentes dispositivos, a través de diversas redes de comunicación, para la prestación de una amplia variedad de servicios, aplicaciones, y contenidos digitales, todo ello en un entorno distribuido y con capacidad de interacción con los usuarios.

Las Tecnologías de la Información y la Comunicación (TICs) son, sin lugar a duda, una de las herramientas más útiles en el desarrollo de las aplicaciones de la Inteligencia Ambiental (AmI) cuyo principal objetivo es el de favorecer y dar soporte a la mayoría de las actividades que realizamos a diario. Las innovaciones desarrolladas a nivel de las tecnologías de la información y las comunicaciones en las dos últimas décadas han permitido el desarrollo de una gran cantidad de aplicaciones en el ámbito de la Inteligencia Ambiental, que han impactado de manera considerable en la operativa de los negocios, las empresas, la administración de los gobiernos, la educación, la salud, el ocio y entretenimiento, etc. impactando, sobre todo, en las diferentes actividades personales que realizamos de forma cotidiana, lo cual nos lleva a tener en consideración ciertas implicaciones sociales y éticas.

La convergencia de ordenadores ubicuos insertados en objetos cotidianos, las comunicaciones inalámbricas entre ellos, los interfaces de nueva generación, los sensores biométricos, los agentes inteligentes, los sistemas de personalización, los ordenadores emocionales, la nanotecnología, la vida artificial, los sistemas de inmersión virtual, el papel electrónico, la bioclimática activa, etc. conforman un nuevo escenario tecnológico con una gran proyección de futuro: la Inteligencia Ambiental que nos rodeará y aumentará nuestras capacidades cognitivas. "*En nuestro futuro*

inmediato la inteligencia penetrará en el entorno, y se convertirá en una presencia ambiental" [Eli Zelkha and Epstein B. 1998].

El gran impacto de la Inteligencia Ambiental se debe al hecho de haber sido denominada, por la Comisión Europea, como el principal escenario de futuro para el siglo XXI a través del Programa Conjunto Ambient Assisted Living-AAL169. En este programa se establecen las pautas a seguir en el campo de la investigación europea durante el período 2003-2006, siguiendo las directrices indicadas por el ISTAG (Information Society Technologies Advisory Group) en lo que se refiere al desarrollo de la Inteligencia Ambiental *[ISTAG 2001] [ISTAG, 2002]*. Por otra parte, en el borrador del Séptimo Programa Marco aprobado a finales de 2006 que determina las pautas de la investigación europea para el período 2007-2013, sigue considerándose como prioritaria la investigación en Inteligencia Ambiental *[7PM]*. Tras las investigaciones realizadas por la comisión europea en estos años, podemos decir que, desde el año 2010, la Inteligencia Ambiental ha pasado a formar parte activa de nuestra vida cotidiana. Conviene destacar que la investigación y el desarrollo del concepto de Inteligencia Ambiental no tienen como objetivo únicamente la creación de entornos inteligentes aislados, sino que aspiran a lograr espacios inteligentes ubicuos que sean capaces de cubrir todos los ámbitos en los que se desarrolla la vida de los usuarios. Este es el concepto definido por el ISTAG como "*Espacio de Inteligencia Ambiental*" *[ISTAG, 2003]*. El Programa Marco de Investigación e Innovación de la Unión Europea Horizonte 2020 *[H2020]*, para el periodo 2014-2020, continúa con las investigaciones dirigidas al bienestar de los ciudadanos europeos, entre las que se encuentra el envejecimiento de la sociedad y la protección informática.

La visión de la Inteligencia Ambiental supone un salto cualitativo, lejos de los ordenadores tradicionales, hacia una amplia variedad de dispositivos de computación y comunicación, inmersos de manera no intrusiva en nuestro entorno, a los que accedemos a través de interfaces inteligentes como: tarjetas de identificación por radiofrecuencia (RFID), tecnología NFC (Near Field Computing), redes de sensores inalámbricos (WiFi, Bluetooth, etc.), dispositivos móviles (PDA, Smartphone, etc.), dispositivos computacionales alojados en nuestra ropa o cuerpo, etc.

Por ello, la mayoría de las interacciones que se desarrollan en Inteligencia Ambiental, aparecen inmersas en objetos cotidianos y dispositivos inteligentes en los que, en ocasiones, se encuentran integrados el mundo físico y el mundo digital. Las diferentes interacciones que tienen lugar en los dominios de aplicación del AmI se basan en entradas e interacciones multimodales, en las que los usuarios acceden de diversas formas como pueden ser: el habla, el tacto, los gestos, el movimiento de los ojos, cabeza o cuerpo, el ratón, el teclado, etc., y en las que suele haber más de una salida modal, siendo las más comunes la visual, la sonora y la mecánica; y todo ello en un contexto dinámico, distribuido y adaptativo que, de manera natural, ofrece al usuario la forma de interactuar más apropiada según el dominio en el que se encuentre, y según sus necesidades o preferencias, facilitándole, de esta forma, llevar a cabo gran parte de las actividades que realiza de forma habitual.

Las tecnologías y dispositivos utilizados en los dominios de aplicación de la Inteligencia Ambiental presentan la característica de poder entender y satisfacer las necesidades de los usuarios, tanto a nivel personal como colectivo, gracias a su capacidad de computación y de comunicación, permitiéndoles así adquirir, almacenar, gestionar y transmitir diferentes tipos de información, a la vez que establecen comunicación con el usuario.

Del mismo modo que la World Wide Web ha cambiado nuestra manera de comunicarnos y el modo en el que compartimos información, la Inteligencia Ambiental está influyendo de manera notable en nuestras vidas, llegando en muchos casos a determinar la forma de percibir, comunicar y modelar nuestra propia identidad; situándonos en el centro de un entorno computacional dinámico y totalmente adaptativo.

Desde las dos últimas décadas, las nuevas tecnologías y el uso de la información nos están ofreciendo, sin duda, grandes beneficios tanto a nivel social como a nivel económico. El volumen de diferentes tipos de información y datos personales que son recogidos, almacenados y utilizados es sumamente amplio, encontrándose además en continuo crecimiento. Gracias a las nuevas redes de comunicación, disponemos de un

acceso globalizado a la información de una manera continua y a través de distintos puntos de conexión que nos permite además la transmisión de la misma entre diferentes partes.

Por este motivo, las aplicaciones desarrolladas en Inteligencia Ambiental no solo han de ir dirigidas a facilitar la realización de nuestras actividades cotidianas, sino que deben también ser utilizadas para proteger nuestros datos e información personal, ayudándonos de esta forma a garantizar nuestro derecho a la intimidad.

Uno de los grandes objetivos de las tecnologías del AmI (por definición) es que resulte invisible para el usuario, pero teniendo en cuenta que la adquisición, almacenamiento, gestión y transmisión de los datos o información que se obtienen a través de las aplicaciones desarrolladas en AmI suponen un riesgo para nuestra privacidad, consideramos que lo que debería ser es transparente, es decir, el usuario ha de saber que dicha tecnología está presente cuando accede a un determinado servicio o aplicación.

Esta transparencia de las diferentes tecnologías utilizadas en las aplicaciones del AmI no debe centrarse solo en el punto de vista de su usabilidad, sino que debe facilitar al usuario el conocimiento de que dicha tecnología está presente en un determinado contexto o dominio de aplicación, para que, de esta forma, el usuario sea consciente de qué tipo de control y gestión sobre sus datos o información personal se está realizando al acceder a un determinado servicio o aplicación del AmI; y todo esto debe hacerse de una manera lo más accesible y fácil posible, con independencia del nivel o capacidad de comprensión del usuario.

No resulta fácil saber si nuestros datos e información personal, al acceder a las tecnologías de la información y la comunicación, y en especial a las aplicaciones desarrolladas dentro de la Inteligencia Ambiental, están realmente protegidos, pero podemos intentar minimizar los riesgos que amenazan nuestra privacidad.

El uso de las tecnologías y servicios ofrecidos por la Inteligencia Ambiental no debe suponer una amenaza o riesgo para la privacidad de los datos o información del usuario, sino que, por el contrario, deben ayudar a preservarla.

Por este motivo, resulta fundamental que en el desarrollo de las aplicaciones de la Inteligencia Ambiental no dejemos de lado sus implicaciones sociales y éticas, sino que utilicemos las tecnologías presentes en los entornos del AmI para ayudarnos a proteger nuestro derecho a la privacidad.

1.2. INTELIGENCIA AMBIENTAL (AmI)

1.2.1. Aproximación al concepto y origen del AmI

El concepto de Inteligencia Ambiental (AmI) ha sido descrito desde distintas perspectivas. Desde un punto de vista psicológico, podemos definir la Inteligencia Ambiental como "el soporte eficaz y transparente para la actividad de los sujetos a través del uso de las tecnologías de la información y las comunicaciones". Otra definición, más tecnológica, describe la Inteligencia Ambiental como "una inteligencia omnipresente y transparente en un entorno vigilado que ayuda a la realización de las distintas actividades e interacciones de los usuarios". Teniendo en cuenta ambas aproximaciones, podemos definir la Inteligencia Ambiental como un entorno provisto de dispositivos electrónicos que son sensibles y responden a la presencia de las personas de una manera inteligente y oculta para el usuario. La Inteligencia Ambiental engloba una serie de dispositivos electrónicos inteligentes que son sensibles y responden a la presencia de las personas *[E.H.L. Aarts et al. 2001].*

Los principales aspectos que caracterizan las aplicaciones desarrolladas en AmI son: por un lado que las tecnologías y dispositivos utilizados se encuentran inmersos en objetos utilizados en nuestra vida cotidiana, llegando a veces a ser totalmente invisibles; y por otro lado que las interfaces de usuario desarrolladas para ofrecer los servicios del AmI han de ser lo más sencillas que sea posible, proporcionando una interacción con el usuario de la manera más natural.

En resumen, podemos considerar la Inteligencia Ambiental como un modelo de interacción entre las personas y el entorno digital que las rodea, caracterizado por tener consciencia de la presencia de los usuarios, ser sensible al contexto y ser capaz de responder adaptándose a nuestras necesidades, hábitos y/o preferencias, facilitándonos muchas de las actividades que realizamos en nuestra vida diaria en diferentes entornos como el hogar, el trabajo, los lugares de ocio, etc.

En la historia de la Inteligencia Ambiental, existen dos conceptos fundamentales que la definen a ambos lados del Océano Atlántico: La Computación Ubicua (en el lado americano), y la Inteligencia Ambiental (en el lado europeo).

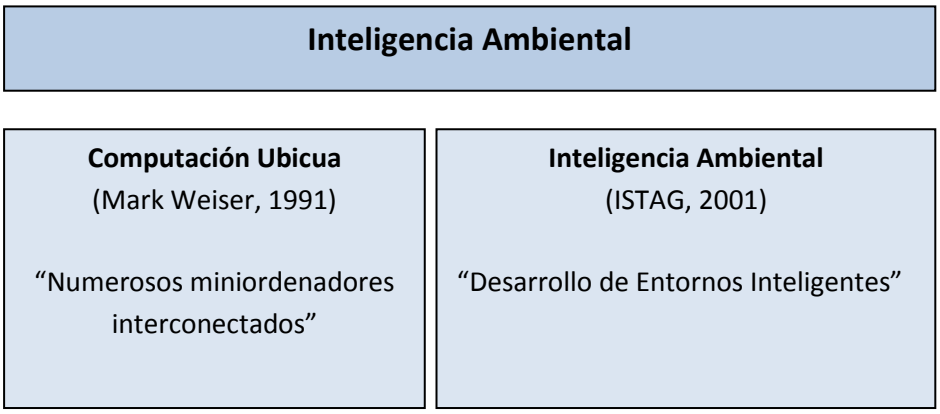

Figura 1.1. Definiciones del AmI

1.2.2. Computación Ubicua

La visión de la Inteligencia Ambiental se basa en las ideas de Computación Ubicua que fueron introducidas en 1990 por Mark Weiser, quien, tras aprovechar los resultados obtenidos en su laboratorio Xerox Parc Lab de California (a mediados de los años 80), en los que elaboró el primer escenario de AmI (cientos de pequeños ordenadores interconectados que pasaban prácticamente inadvertidos en forma de insignias, tarjetas y pizarras electrónicas), anticipó que en el futuro estaríamos rodeados por un mundo digital en el que los dispositivos electrónicos estarían inmersos en complejas redes distribuidas *[M. Weiser, 1991-1992].*

Para Mark Weiser, la Computación Ubicua representa la tercera etapa dentro de la evolución de la informática. En la primera etapa existían los grandes ordenadores o mainframes que eran compartidos por una gran cantidad de personas (un ordenador para muchas personas), en la segunda etapa aparecieron los ordenadores personales, (un ordenador para cada persona), y en la tercera etapa que según Weiser se desarrollaría en un futuro cercano, cada persona interactuará con una gran cantidad de ordenadores (muchos ordenadores para cada persona). Su proyección del futuro era que *"estos ordenadores ubicuos deberán saber en qué lugar se encuentran para adaptarse al entorno e identificarán a su usuario mediante un sistema de búsqueda por radiofrecuencia internacional"*.

De acuerdo con estas ideas, Mark Weiser consideraba que la verdadera revolución tecnológica iría dirigida a que los dispositivos fueran cada vez más pequeños e invisibles. Su idea de futuro consistía en que viviríamos rodeados de centenares de pequeños ordenadores insertados en objetos cotidianos de nuestro entorno, y que podrían analizar tanto el entorno como a los usuarios y tendrían, además, la capacidad de anticiparse a nuestros deseos haciendo el entorno más inteligente y accesible para todos. Mark Weiser llegó a considerar a la Inteligencia Ambiental como el nuevo paradigma de la computación con mayor expansión y con mayores posibilidades de impacto social y económico que marcaría, al menos en parte, el futuro de la Informática en las siguientes dos décadas.

Después de más de dos décadas en las que se han producido grandes avances tecnológicos dentro del ámbito de los sistemas de información y de la comunicación, nos encontramos con el hecho de que muchos de los dispositivos electrónicos que fueron ideados por Weiser, son ahora productos comerciales que utilizamos en la mayoría de las actividades que realizamos habitualmente: Smartphone, Networks, Wireless data, Terminales multimedia, Pas, LAN's inalámbricas, Sensores inteligentes, etc.

1.2.3. Inteligencia Ambiental

Las compañías americanas Palo Alto Ventures y Silicon Artists, en 1998 y bajo la dirección de Roel Pieper y la subdirección de Stefano Marzano (actual director ejecutivo de Philips Design), reunieron a un grupo de expertos de distintas empresas e institutos de investigación de todo el mundo como el MIT (Massachusetts Institute of Technology) para conceptualizar la visión de que varios ordenadores ubicuos interconectados serían capaces de aprender de sus usuarios y, así, mejorar la vida de las personas.

Este grupo de expertos llamado ISTAG "Information Society Technologies Advisory Group" presentó en el año 2001 un informe a la Information Society Directorate General (perteneciente a la Comisión Europea) en el que incluyeron el concepto y el escenario del Ambient Intelligence (AmI). En dicho informe, definieron la Inteligencia Ambiental como una novedosa línea de investigación consistente en la creación de espacios habitables a los que denominaron "Entornos Inteligentes", en los cuales los usuarios podían interactuar de manera natural e intuitiva con diferentes servicios computacionales que les permitían realizar sus tareas diarias de una manera más fácil. Así pues, las aplicaciones del AmI incluyen una extensa e invisible integración de tecnologías computacionales presentes en la vida diaria de los usuarios *[ISTAG, 2001].*

La compañía Philips inició sus investigaciones sobre Inteligencia Ambiental en el Home Laboratory, al tiempo que otras compañías e instituciones tecnológicas hicieron lo mismo, todo ello con el propósito de mejorar la calidad de vida de la sociedad. A partir de entonces, Philips ha seguido liderando este campo y presentando aplicaciones concretas inspiradas en esta visión, que han sido englobadas en la presentación comercial de "La Casa conectada" mostrada en 2003 en el Ce Bit Rudy Provoost, actual CEO de Philips Electronic Consumer.

Con las ideas planteadas por el grupo ISTAG, por primera vez el ser humano no tendría que adaptarse a las máquinas, sino que sería la tecnología la que se adaptaría a él. "*La inteligencia penetrará en el entorno como una presencia ambiental, entorno en el que nuestras necesidades se verán satisfechas del mismo modo en que la sangre circula en nuestro cuerpo: sin mediar una orden consciente*", decían estos pioneros en su libro blanco.

Teniendo en cuenta esta visión de la Inteligencia Ambiental, podemos decir que los "Entornos Inteligentes" desarrollados en Inteligencia Ambiental tienen como objetivo fundamental proveer servicios personales a los usuarios para facilitarles el desarrollo de sus actividades cotidianas.

1.2.4. Características del entorno del AmI

Las diferentes tecnologías de computación y comunicación presentes en Inteligencia Ambiental permiten la creación de espacios donde los usuarios interaccionan de manera natural y sencilla con los distintos sistemas que los conforman. En estos entornos, las tecnologías del AmI se vuelven invisibles para el usuario, estando presentes e integradas en diversos objetos de su vida cotidiana. De esta forma, la propia tecnología se adapta al usuario y al contexto en el que se encuentre, facilitándole la realización de sus tareas diarias, a la vez que permite la comunicación entre el usuario y el entorno inteligente que le rodea. Por ello, resulta de gran interés el uso de las tecnologías de la computación para la construcción de estos sistemas que son capaces de dar soporte, de la manera más eficiente posible, a las diferentes actividades habituales de los usuarios, entre las que podemos destacar: el control del hogar, el cuidado de la salud, las tecnologías de asistencia, la educación, la actividad laboral, los negocios, el ocio y el entretenimiento.

La Inteligencia Ambiental puede caracterizarse como un entorno digital inteligente y embebido que es sensible y responde a la presencia de las personas *[Gaggioli, A. 2005]*. Es decir, la Inteligencia Ambiental se caracteriza por tener una gran cantidad de objetos inteligentes, distribuidos y conectados entre sí por diversas tecnologías, con sus correspondientes protocolos de comunicación, que conforman un entorno o

ambiente inteligente. Estos dispositivos inteligentes, además, son sensibles al entorno, poseen la capacidad de obtener datos e información tanto del usuario como del entorno que le rodea, siendo también capaces de controlar este entorno e interactuar con los usuarios, todo ello de una forma natural y muchas veces imperceptible (computación invisible) para los usuarios.

Los entornos de Inteligencia Ambiental pueden ser implementados en diferentes escenarios o dominios, entre los que tenemos: Escenarios domésticos, espacios móviles (coche, autobús, tren, avión, etc.), entornos públicos (oficinas, tiendas, museos, hospitales, etc.) e incluso en espacios privados reducidos (ropa inteligente), dando así servicio al usuario en cualquier dominio en el que se encuentre desarrollando alguna actividad. Así, la propia tecnología presente en los entornos de Inteligencia Ambiental se adapta al usuario y a su contexto, facilitándole la realización de sus tareas cotidianas, siendo a veces capaz de actuar de manera autónoma.

En *[E.H.L. Aarts et al. 2001]*, los autores establecieron las principales características que debe tener un sistema en Inteligencia Ambiental para desarrollar el enfoque de la "computación invisible" *[Schmidt, 2005]*:

- *Discreción*. Los dispositivos deben ser invisibles tanto física como psicológicamente.
- *Personalización*. El sistema o entorno inteligente ha de reaccionar de acuerdo a la situación y perfil de cada usuario.
- *Adaptabilidad*. Los dispositivos han de tener la capacidad de modificar el entorno en función de la información del mismo y del usuario.
- *Pro-actividad*. Deben ser capaces de prever la mayor cantidad de procesos posibles en el entorno.

Basándose en estos principios, definieron la Inteligencia Ambiental como la sinergia de tres atributos:

- *Ubicuidad*. El entorno se encuentra enmarcado por múltiples dispositivos embebidos e interconectados.
- *Transparencia*. La tecnología es invisible y está integrada en el entorno del usuario.
- *Inteligencia*. El entorno tiene la capacidad de reconocer a las personas que se encuentran en él, de adaptarse y aprender de su comportamiento.

Podemos así calificar un entorno como inteligente cuando, de manera no intrusiva, disponga de diversas tecnologías presentes alrededor de los usuarios que sean capaces de proporcionarles los servicios y prestaciones que les soliciten, o que sean predecibles de ser solicitados en cualquier ámbito en el que los usuarios se encuentren desarrollando alguna actividad. Por ello, un entorno inteligente deberá disponer de una serie de tecnologías que sean capaces de:

- Relacionarse con naturalidad con los usuarios mediante interfaces multimodales.
- Reconocer a los usuarios y su contexto para actuar en consecuencia, es decir, debe ser sensible a la presencia de las personas.
- Tener un comportamiento predictivo de los hábitos de los usuarios a partir del conocimiento del entorno “context awareness”, así como de las actividades concretas que se encuentren realizando los usuarios y ofrecerles sus servicios.
- Proporcionar en tiempo real servicios en diferentes ámbitos o dominios, como: el entretenimiento, la seguridad, la salud, el trabajo doméstico, el entorno laboral, etc., que mejoren la realización de las diferentes tareas que realiza el usuario de manera cotidiana.

- Permitir que el acceso a los servicios ofrecidos pueda llevarse a cabo independientemente del lugar en el que se encuentre el usuario (ubicuidad de actuación), de cuándo solicite dichos servicios, y de los dispositivos que tenga disponibles en ese momento.

Todas estas capacidades no sólo establecen las principales características que deben cumplir las tecnologías presentes en la Inteligencia Ambiental, sino que además definen las principales líneas de investigación que deben llevarse a cabo para el desarrollo de los entornos inteligentes, como son:

- La comunicación y la computación deben ser transparentes para el usuario, y han de centrarse en el modo de interaccionar con las personas, facilitando así la realización de servicios ofrecidos sin necesidad de la intervención humana.
- Los entornos y dispositivos deben ser desarrollados para múltiples usos en aplicaciones de entornos físicos heterogéneos.
- Todos los servicios ofrecidos deben estar siempre disponibles, en cualquier momento y en cualquier lugar.

Las propiedades de la Computación Ubicua: portabilidad, redes con conectividad inalámbrica, localización sensible, seguridad, interoperabilidad, ser distribuida y escalable, presentadas en *[F. Adelstein et al. 2004],* proporcionan un nuevo enfoque sobre la computación móvil, ya que tanto los dispositivos móviles como los servicios que estos ofrecen se encuentran disponibles en cualquier momento y lugar, creando un ambiente inteligente integrado en objetos y entornos cotidianos en los que se desarrollan diferentes formas de interacción socio-digital, que presentan capacidad de reconocimiento de las personas, llegando a personalizar los servicios disponibles de acuerdo con las preferencias de los usuarios.

Teniendo en cuenta las capacidades y características mencionadas anteriormente, y considerando el hecho de que en los dominios de la Inteligencia Ambiental tienen lugar distintos tipos de interacción socio-digital, podemos establecer cuáles son las características principales que debe tener un sistema, tanto desde el punto de vista tecnológico como desde el punto de vista social y ético, para desarrollar la visión de la Inteligencia Ambiental:

- *El entorno debe ser sensible al contexto.* Es decir, el entorno ha de tener consciencia del contexto, lo que significa que ha de tener capacidad de reconocer el contexto en el que se encuentra para poder adaptarse a la información proveniente del mismo, responder en consecuencia y aprender.

- *Dispositivos inmersos en el ambiente*. El acceso a la información, a la comunicación y a los servicios, debe realizarse de forma ubicua, inalámbrica y transparente para el usuario. Para ello, resulta necesario el desarrollo de nuevas técnicas de miniaturización y la utilización de nuevos materiales que permitan crear hardware cada vez más pequeño. Estos dispositivos han de adaptarse a las necesidades o solicitudes de los usuarios y han de poder anticiparse a los requerimientos de los mismos.

- *Infraestructura de comunicaciones fija y móvil*. Los dispositivos presentes en el entorno inteligente son heterogéneos y necesitan una infraestructura de comunicaciones que permita su integración total. De esta forma, se podrán dispositivos electrónicos de cualquier tipo: sensores, cámaras, procesadores, tarjetas inteligentes, electrodomésticos, Smartphone, etc.

- *Redes dinámicas de dispositivos distribuidos*. La red que permita la comunicación entre los dispositivos, debe ser dinámica para que pueda reconfigurarse de manera automática en cualquier momento en el que se añada o elimine alguno de los dispositivos.

- *Interfaz natural e intuitiva*. La interacción entre el usuario y el sistema debe realizarse de forma sencilla, natural y no intrusiva (la tecnología debe adaptarse a las personas). Para ello, resulta necesario el desarrollo de middleware que sirva de intermediario entre el usuario y los diferentes dispositivos.

- *Fiabilidad, seguridad y privacidad*. El entorno inteligente obtiene información personal del usuario al interaccionar y comunicarse con él para ofrecerle un servicio personalizado. Por ello, no sólo es importante que esta información sea fiable y segura, sino que debe garantizarse también la privacidad de la misma.

1.2.5. Fundamentos de la Inteligencia Ambiental

El objetivo final de la Inteligencia Ambiental es el de facilitar y mejorar la vida de las personas, de tal forma que permite la realización de las diferentes tareas que forman parte de nuestra vida cotidiana de la manera más inteligente posible, ayudándonos así a llevar una vida más cómoda y fácil. Un entorno o ambiente será más inteligente cuanto más ayude a los usuarios a desarrollar sus capacidades tanto cognitivas como de actuación.

Basándonos en esta idea, y considerando las características socio-tecnológicas principales que debe tener un sistema para desarrollar la visión de la Inteligencia Ambiental (descritas en el apartado anterior), detallamos a continuación cuáles son los principales componentes que intervienen en un ambiente inteligente (tanto en la capa tecnológica como en la capa social), y que son los que conforman los fundamentos sobre los que debe asentarse la Inteligencia Ambiental en el desarrollo de sus aplicaciones.

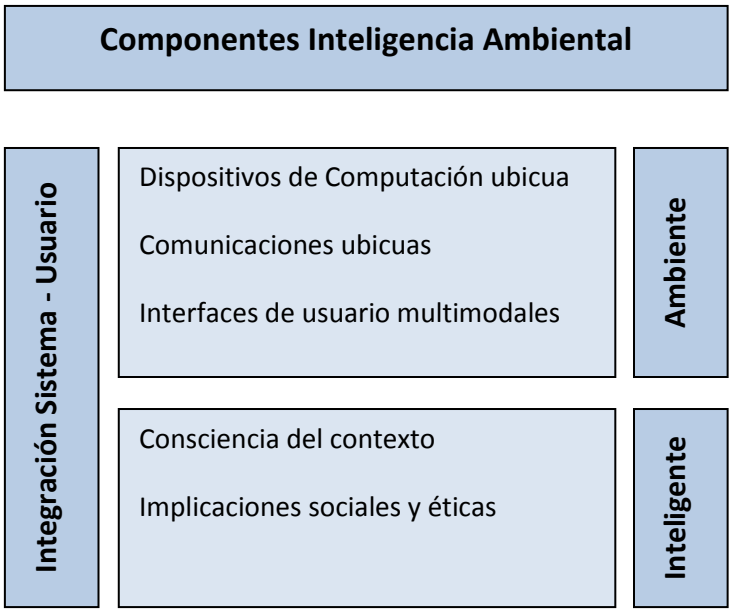

Figura 1.2. Componentes socio-tecnológicos del AmI

1.2.5.1. Dispositivos de Computación ubicua

Las principales características de la computación ubicua son la omnipresencia y la transparencia del sistema. Podemos definir un sistema ubicuo como un espacio en el que se encuentran implementados diferentes dispositivos electrónicos (con capacidad computacional), conectados a través de una red, alrededor del usuario, y con capacidad de interactuar con él. Todos estos dispositivos computacionales que se encuentran distribuidos de forma masiva necesitan estar disponibles en cualquier lugar y en cualquier momento, para comunicarse entre ellos y con los usuarios de la manera más discreta y fácil posible, y utilizando el entorno físico como su interface *[Punie, 2003]*.

El creciente desarrollo y expansión de la tecnología de computación ubicua ha llevado a definir el concepto de "everywhere" como el procesado de la información integrado en los objetos y superficies de la vida cotidiana *[Adam Greenfield, 2006]*, en cualquier lugar y momento.

Las capacidades más relevantes que presentan los dispositivos de computación ubicua para desarrollar la visión del AmI son, por una parte, analizar tanto al usuario como al entorno que le rodea adaptándose en consecuencia, y por otra parte, llegar incluso a anticiparse a los diferentes servicios o necesidades que pueda necesitar o solicitar el usuario. Los dispositivos computacionales capturan las experiencias diarias del usuario mediante la monitorización y recogida de la información asociada al entorno en el que se encuentra (información de contexto), y acceden tanto a la información del propio sistema, como a cualquier tipo de información nueva que pueda obtenerse del exterior (Internet), desde cualquier lugar y en cualquier momento. Otra de las capacidades de las que deben disponer estos dispositivos computacionales es la de dar soporte a la comunicación y colaboración, así como la de desarrollar entornos sensibles al contexto que permitan obtener tanto la información del entorno como la del usuario, procesarla, y en función del análisis de esta información, ser capaces de modificar su comportamiento. Para el desarrollo de estas capacidades, se necesita que esos dispositivos tengan unos requerimientos básicos como son: disponer de procesamiento específico, flexibilidad, robustez, facilidad para la sincronización, bajo consumo energético, tamaño reducido y seguridad.

Las redes de sensores inalámbricos destacan como uno de los dispositivos computacionales más utilizados en los dominios de aplicación del AmI en la obtención de información del entorno del usuario y su posterior tratamiento, para ofrecer los servicios solicitados por el usuario. Esta información puede provenir del propio usuario como son los datos fisiológicos (presión sanguínea, ritmo cardiaco, niveles de azúcar y de oxígeno, etc.), de su comportamiento (sensores de detección de presencia, de detección de caídas, etc.), o del entorno que le rodea (temperatura, humedad, luminosidad, sonoridad, humo, etc.).

Estas redes de sensores inalámbricos están formadas por una serie de unidades autónomas (nodos) que constan de un micro-controlador, una fuente de energía (generalmente una batería), un radio-transceptor (RF) y un elemento sensor.

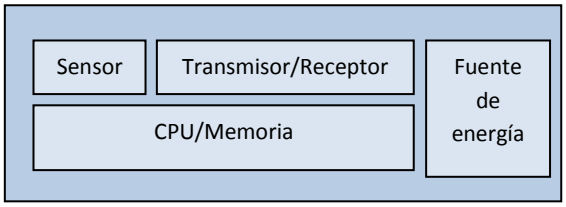

Figura 1.3. Componentes de un nodo sensor

Atendiendo a la información obtenida del entorno, estos sensores pueden ser clasificados en cuatro grandes grupos:

- *Sensores vitales*. Destinados a la obtención de parámetros vitales del usuario (detectan actividad nerviosa y muscular).

- *Sensores biométricos*. Utilizados para el reconocimiento o identificación en tiempo real del usuario que ocupa un entorno, mediante el análisis de sus características biométricas (modulación de la voz, iris del ojo, gestos habituales, huellas dactilar y/o digital, etc.).

- *Sensores de comportamiento*. Obtienen información sobre el estado, ubicación y forma de actuar de los usuarios, en un ámbito más general y no orientado a parámetros vitales, con el objetivo de detectar cambios de su situación inicial o anomalías. Entre estos sensores de comportamiento destacan los sensores de localización, los sensores de detección de caídas y los dispositivos de aviso de socorro.

- *Sensores ambientales*. Se encargan de capturar la información del entorno del usuario para poder saber si el entorno se encuentra dentro de los parámetros ambientales correctos, y sin riesgo para el usuario. En este tipo de sensores se encuentran los sensores ambientales y los sensores de detección de peligro.

La mayoría de los dispositivos de computación ubicuos son portables y presentan la capacidad de poder comunicarse entre ellos y con el usuario. En la actualidad, podemos ya encontrarlos inmersos en muchos objetos cotidianos de nuestra vida conocidos como "sistemas embebidos" (mesas, paredes, bolígrafos, tarjetas de crédito, electrodomésticos, Smartphone, etc.), cuyo desarrollo en los últimos años ha dado lugar a la llamada "cultura celular" que nos permite llevar una minicomputadora en nuestros bolsillos. Gracias a la ubicuidad de la tecnología de la computación, podemos encontrar todos los sistemas de información integrados en la mayoría de los objetos que utilizamos a diario, volviéndose invisibles o imperceptibles para el usuario, de tal forma que éste no es consciente de su presencia, lo cual supone un importante impacto social que lleva a plantear el reto de establecer la necesidad de ser conscientes de su presencia y poder así darle un uso adecuado.

1.2.5.2. Comunicaciones ubicuas

Todos los dispositivos computacionales que forman parte de un entorno inteligente tienen la capacidad de interactuar entre sí y con el usuario, por lo que necesitan el desarrollo de una comunicación ubicua que permita a los usuarios el acceso a los servicios computacionales ofrecidos por el sistema, en cualquier momento y desde cualquier lugar. Las comunicaciones ubicuas proporcionan información a los usuarios, a través de los diferentes dispositivos computaciones que se encuentran dispersos en el entorno por lo que, de esta forma, se minimiza la intervención explícita de los usuarios.

En *[Nava & Bravo, 2007]*, se detallan cuáles son las características que deben tener las comunicaciones ubicuas:

- Obtener solamente la información que se necesita. Los sistemas deben ser capaces de ofrecer al usuario únicamente la información concreta e imprescindible.

- La comunicación ha de ofrecerse en el momento y lugar que se requiera. La información debe ser proporcionada de la manera más rápida posible para que, de esta forma, facilite el que sea utilizada dentro del contexto donde se solicitó y en cualquier lugar.

- Deben realizarse de una manera sencilla e inmediata. La interacción del usuario con el sistema debe ser sencilla, para que de esta forma interactúe lo menos posible con los dispositivos computacionales, y sólo tenga que intervenir cuando sea necesario; proporcionando la información solicitada sin demoras innecesarias.

- Tienen que darse sin gasto energético excesivo. Los dispositivos móviles no deben realizar demasiados procesos, para que no utilicen innecesariamente la batería.

- Deben favorecer la movilidad. El entorno debe ser capaz de seguir proporcionando el servicio incluso si el usuario se encuentra fuera del lugar donde inició la petición de la información.

Teniendo en cuenta todas estas características, podemos decir que la comunicación ubicua se fundamenta principalmente en la implementación de redes inalámbricas que nos van a permitir la comunicación y transmisión de datos e información entre los diferentes dispositivos computacionales de nuestro entorno, entre ellos y con nosotros como usuarios. De esta forma se consigue tener disponible un mayor número de servicios y de mejor calidad.

Red	Descripción	Distancia	Tecnología
Red de Área Corporal (BAN)	Sensores, chips o dispositivos electrónicos integrados en la ropa, o situados en alguna parte del cuerpo del usuario.	~ 1 metro	Sensores, Interfaces.
Red de Área Personal (PAN)	Red formada por la interconexión de todos los dispositivos personales móviles que el usuario lleve consigo.	~ 10 metros	Dispositivos de Entrada/Salida, Periféricos.
Red de Área Local (LAN)	Ofrecen acceso tanto a las redes fijas y móviles como a Internet.	~ 100 metros	Puertos de comunicación.
Red Área Ampliada (WAN)	Redes que ofrecen mayor alcance para facilitar la movilidad total del usuario.	Mundo	Enrutamiento y protocolos de transporte.
Mundo Virtual	Red formada por todos los elementos presentes en el entorno, sin límites teóricos.	Universo	Comunicación teórica entre agentes.

Tabla 1.1. Niveles de redes utilizadas en AmI

En la tabla presentada se muestran las redes de comunicación que se utilizan generalmente en las aplicaciones de Inteligencia Ambiental, *[Riva, Loreti, Lungui, Vatalaro & Davide, 2003]*.

Entre los principales protocolos de comunicación inalámbrica que se encuentran más consolidados para dar soporte a la Computación ubicua, destacamos los siguientes: WiFi, WiMAX, ZigBee, GPRS/GSM, Redes 3G/UMTS, Bluetooth, IRDA, RFID, TETRA.

- *WiFi* (*Wireless Fidelity,* utilizado desde 1999). Esta tecnología de comunicación inalámbrica mediante ondas es la más utilizada hoy en día, por lo que uno de los problemas a los cuales se enfrenta actualmente es la progresiva saturación del espectro radioeléctrico debido a la masificación de usuarios, que afecta especialmente en las conexiones de larga distancia (alcance medio de 150 m). El mayor inconveniente de las redes WiFi en el entorno del AmI es que son bastante vulnerables, a nivel de seguridad, en la transmisión de los datos.

- *WiMAX (Worldwide Interoperability for Microwave Access)*. Esta norma de transmisión de datos sigue el estándar IEEE 802.16, similar a WiFi pero con mayor cobertura (hasta 50 km) y ancho de banda. En el entorno del AmI, la utilización de esta tecnología permite mejorar la comunicación entre personas residentes en lugares de difícil acceso, optimizando así los recursos sociales para la comunicación, al evitar el desplazamiento de este colectivo fuera de su entorno.

- *ZigBee* (utilizado desde 2004). Se trata de un estándar inalámbrico que emplea señales de radio de corto alcance, minimizando así el consumo de energía y alargando la vida útil de las baterías. En los entornos inteligentes del AmI, se suele utilizar principalmente para la comunicación de redes dedicadas a la monitorización y dispositivos de control. Esta tecnología ofrece un alto nivel de seguridad en las comunicaciones con baja tasa de transmisión de datos, destacando en la actualidad por su reducido consumo sobre otras como WiFi o Bluetooth, y por ofrecer múltiples tipologías de red con gran nivel de integración. La utilización de esta tecnología en los entornos inteligentes del AmI resulta muy apropiada, ya que permite un funcionamiento continuo/periódico, además de la posibilidad de trabajar por eventos. Entre otras ventajas que presenta esta tecnología de comunicación para ser implementada en diferentes tipos de sensores integrados en los entornos inteligentes, destacan: es una tecnología de comunicación económicamente accesible, resulta fácil de instalar, mantener y utilizar (redes tipo ad-hoc auto-configurables, que pueden expandirse fácilmente), es flexible y modular,

fácilmente adaptable al entorno, robusta y fiable, y resulta mínimamente invasiva de la intimidad de los usuarios.

- *GPRS/GSM (*General Packet Radio Service/Global System for Mobile Communications). Tecnología de comunicación digital utilizada en telefonía móvil de segunda generación (2.5G y 2G) para el envío y recepción de datos, mediante la asignación de canales de frecuencia de radio. Uno de sus mayores inconvenientes es la baja velocidad en la transmisión de la información.

- *Redes 3G/4G/5G UMTS (Universal Mobile Telecommunications System)*. Esta tecnología de comunicación, sucesora de la tecnologías GPRS/GSM, representa la tercera, cuarta y quinta generación en la transmisión de voz y datos a través de la telefonía móvil, ofreciendo mayor velocidad y facilitando la transmisión de información más compleja como puede ser el envío y procesado de vídeos. A diferencia de los protocolos ZigBee, Bluetooth o WiFi, este tipo de tecnología es capaz de ofrecer comunicación inalámbrica en áreas extensas, gracias a la utilización de la cobertura de la telefonía móvil.

- *Bluetooth* (desde 1994). Esta especificación define un estándar de comunicación inalámbrica, para la formación de redes de área personal o PAN en la transmisión de información a cortas distancias, mediante el uso de señales de radiofrecuencias (alcance aproximado de 10 m).

- *IRDA*. Este tipo de tecnología permite a los dispositivos que la integran comunicarse entre sí (en una distancia de pocos metros) por medio de luz IR, lo cual resulta muy económico.

- *RFID (Radio Frequency IDentification)*. Este estándar de comunicación con capacidad para la identificación entre dispositivos o sensores (emisor/receptor) se basa en señales de radio-frecuencia que no requieren contacto, ni línea de visión directa entre los dispositivos conectados. Los sistemas que integran este tipo de tecnología llevan incorporados una etiqueta que consta de un pequeño microprocesador y una antena, que se activa cada vez que se induce en ella una

señal de radiofrecuencia, lo cual permite la identificación única entre el lector (receptor) y el objeto provisto de esta etiqueta (emisor). Las etiquetas, tarjetas o tags RFID pueden ser de tres tipos: Pasivas (no llevan fuente de alimentación, por lo que solo se comunican cuando son activadas por un lector, alcance aproximado 10 cm), semipasivas (disponen de fuente de alimentación que se utiliza para alimentar el microchip y no para la transmisión de señales), activas (poseen su propia fuente de alimentación que les sirve para comunicarse de manera autónoma, pueden incorporar sensores, alcance hasta 500 m).

- *TETRA (TErrestrian Trunked RAdio)*. Esta tecnología desarrollada por el ETSI (European Telecommunications Standards Institute), constituye un estándar de radio digital móvil que aporta mayor privacidad y confidencialidad, más calidad de audio, así como mejoras en la velocidad de transmisión de datos y en la capacidad de acceso a otras redes como Internet, red telefónica fija o móvil. El uso de las radiocomunicaciones basadas en el estándar TETRA, se encuentra orientado principalmente al ámbito de organismos oficiales (militares, seguridad pública, ambulancias, etc.), que necesitan un alto grado de especialización y fiabilidad en sus comunicaciones, a un coste inferior al de la telefonía móvil GSM. El reducido número de usuarios de este medio de comunicación lo hace especialmente adecuado en el ámbito del Ambient Assisted Living (AAL), ya que su utilización permitiría mejorar la seguridad y fiabilidad en las comunicaciones de este dominio, aumentando así la calidad en la asistencia a los usuarios.

En la siguiente tabla se muestra una comparativa de las tecnologías de comunicación inalámbricas más utilizadas en los entornos inteligentes del AmI, aunque, en la mayoría de los casos, se utilizan varios tipos de redes interconectadas (ejemplo: interconexión de varias redes WPAN).

Tecnología	Estándar	Alcance	Velocidad	Ventajas	Inconvenientes
WLAN (Wireless Local Area Network) - WiFi	IEEE 802.11	2-200 m	11 Mbps (b) 54 Mbps (g)	Estándar consolidado. Amplio alcance. Velocidad y flexibilidad.	Tecnología cara para dispositivos pequeños.
WPAN (Wireless Personal Area Network) - Bluetooth	IEEE 802.15.1	10 m	720 Kbps (v1) 2,1 Mbps (v2)	Estándar consolidado. Bajo coste.	Velocidad baja. Máximo de 8 dispositivos en red.
High Rate WPAN	IEEE 802.15.3	55 m	55 Mbps	Amplio alcance. Bajo coste.	Estándar no consolidado. Mayor consumo que Bluetooth.
Low Rate WPAN-ZigBee	IEEE 802.15.4	75 m	250 Kbps	Consumo mínimo. Bajo coste. Amplio alcance. Fiabilidad.	Tecnología muy novedosa. Velocidad baja.

Tabla 1.2. Comparativa tecnologías inalámbricas en entornos del AmI

En los entornos inteligentes desarrollados en AmI, a la hora de seleccionar la tipología de la red sobre la que se va a transmitir la información, no sólo es necesario considerar los factores físicos como el tamaño de los dispositivos, el alcance de la operación, la velocidad en la transferencia de los datos, etc., sino que resulta fundamental tener en cuenta que la interoperabilidad de los datos que se transmiten se realice de una manera fiable, segura y que tenga en cuenta la protección de nuestra privacidad.

A pesar de que cada fabricante de soluciones tecnológicas en los dominios del AmI emplee formatos de comunicaciones privados para la captura y el envío de la información, puede ocurrir que los datos transmitidos sean visibles y consultados desde otro tipo de dispositivos, por lo que resulta necesario estandarizar la

comunicación de la información para que ésta sea segura y no ponga en riesgo la intimidad de los usuarios.

De acuerdo con este propósito, se han desarrollo distintos estándares como el ISO/IEEE1 1073 (X73) para la interoperabilidad de datos provenientes de dispositivos médicos, o el estándar europeo EN13606 para los registros de salud electrónicos EHR (Electronic Healthcare Record), entre sistemas de información clínica independientes. Sin embargo, en la actualidad, hay un gran número de sistemas desarrollados en Inteligencia Ambiental que no hacen uso de ningún tipo de estándar que garantice la privacidad de la información transmitida.

1.2.5.3. Interfaces de usuario multimodales

Las interfaces de usuario constituyen el tercer pilar sobre el que se fundamenta la Inteligencia Ambiental. Estas interfaces forman un componente esencial en los sistemas desarrollados en AmI, siendo su función principal la de dar soporte a la interacción entre los usuarios y los entornos inteligentes. Lo que hasta hace unos años se conocía como interacción persona-ordenador se contempla en la actualidad como interacción persona-ambiente inteligente, lo cual guarda gran semejanza con la manera de interactuar más natural que es la interacción persona-persona *[Reeves & Nass, 1996]*.

Los autores *[Ferscha A. et al. 2004]* proponen que este tipo de interacción sea espontánea, es decir, los objetos empiezan a interactuar cuando detectan en su proximidad objetos de su interés. Otro concepto propuesto es el de la interacción persistente, que implica la sincronización de la actividad desarrollada por el usuario, incluso si va cambiando el dispositivo computacional con el que está realizando la actividad *[Abowd & Mynatt, 2000].* Otra propuesta que podemos destacar es la de la interacción por contacto; este tipo de enfoque se basa en el acercamiento deliberado de los dispositivos con el fin de obtener servicios *[Chavira, Nava, Hervás, Bravo, & Sánchez, 2007].*

Los autores *[Vincent, V.J. & Francis, K. 2006]* proponen una clasificación de la interacción en función de los flujos de control, distinguiendo tres tipos: interacción en una dirección para aplicaciones que solo requieren mostrar contenidos o bien recibir información de los usuarios; interacción de dos vías, donde la interacción se basa en petición-respuesta; y por último, la interacción de alto grado donde las interacciones son frecuentes en ambas direcciones y no tienen por qué guardar una relación del tipo uno a uno (petición-respuesta).

El concepto de interacción Persona-Ordenador Implícita (iHCI) fue introducido por *[Schmidt, 2005]* en su tesis doctoral, definiéndolo como la *"interacción entre un humano con el entorno y con los dispositivos ideados para lograr una meta, a través de un proceso de adquisición de entradas implícitas y obtención de salidas implícitas"*. Es decir, las entradas implícitas son las acciones y el comportamiento de las personas para alcanzar una meta, de tal forma que el sistema, basándose en esta percepción, es capaz de anticiparse a los deseos del usuario proporcionándole la ayuda necesaria para la tarea que está realizando, en forma de salidas que se encuentran integradas en el mismo entorno.

Las aplicaciones basadas en la interacción implícita propuesta por *[Schmidt, 2005]* presentan una serie de características que las hace idóneas para ser utilizadas en los dominios de la Inteligencia Ambiental:

- Son aplicaciones proactivas y adaptadas al usuario cuyo comportamiento cambia según el contexto, lo cual contribuye a simplificar la tarea del usuario.
- Son interfaces de usuario que se anticipan y muestran los requerimientos del usuario.
- Sirven para actuar como recordatorios.
- Filtran la información en función del contexto.

Los avances desarrollados aplicados en los entornos inteligentes del AmI, en la interacción persona-ordenador, han dado lugar a múltiples trabajos que abordan nuevas técnicas y enfoques sobre las interfaces de usuario, entre los que podemos destacar las aproximaciones que utilizan pantallas táctiles *[Dempski & Harvey, 2006]*, y los sistemas de reconocimiento de gestos y movimientos *[Hervás, R. et al. 2006]*.

Atendiendo a la visión de la Inteligencia Ambiental para que la interacción entre el usuario y el sistema se realice de forma sencilla, natural y no intrusiva (la tecnología debe adaptarse a las personas), podemos destacar las características más importantes que deben tener las interfaces de usuario en el desarrollo de los entornos inteligentes del AmI:

- *Comunicación multimodal*. Las interfaces de usuario inteligentes deben tener la capacidad de comunicarse con el usuario a través de diferentes canales de comunicación, es decir, han de comunicarse con el usuario del sistema de diversas formas como: mensajes escritos, imágenes, habla, gestos, etc. Este tipo de comunicación multimodal permite que la interacción sea más natural y rica que la interacción convencional con el ordenador, que se realiza a través de la pantalla, teclado, o ratón. En la actualidad, se han logrado importantes avances en el desarrollo de interfaces basados en este tipo de comunicación multimodal como: el reconocimiento del habla natural (sentido del oído), el reconocimiento de gestos (sentido de la vista), y la interacción háptica (sentido del tacto).

- *Sensibilidad al contexto*. Las interfaces de usuario multimodales, además de transmitir información interna del sistema, han de ser también sensibles para aprender del entorno y responder en consecuencia. Esto quiere decir que han de tener capacidad de reconocer el contexto en el que se encuentran y recopilar información del mismo, adaptándose a dicha información y poder así, ofrecer a los usuarios los servicios que puedan serle más útiles y adecuados según sus necesidades y/o preferencias.

Entre las interfaces más utilizadas hoy en día, se encuentran las denominadas "wereable computers" que cuentan con capacidades de computación siempre accesibles y que el usuario incorpora en su ropa de forma no intrusiva. Este tipo de dispositivos portátiles ha sido muy utilizado por las tecnologías de la información y comunicación en la obtención de modelos de comportamiento, y en el desarrollo de sistemas de vigilancia de la salud. Presentan una interacción computacional constante con el usuario (en la mayoría de los casos no es necesario encender el dispositivo para que actúe), y poseen capacidad multitarea. Algunos de estos dispositivos pueden ser incorporados en el cuerpo del usuario por medio de prótesis, convirtiéndose así en una extensión de la mente y del cuerpo del usuario.

Las interfaces de usuario multimodales permiten al usuario comunicarse con los diferentes dispositivos computacionales del sistema presente en el entorno inteligente, de una manera sencilla y natural. Estas interfaces ocultan al usuario la complejidad del sistema, mostrándole solamente sus funcionalidades, de esta forma el usuario obtiene el servicio que necesita sin tener que preocuparse de cómo es el funcionamiento interno del sistema.

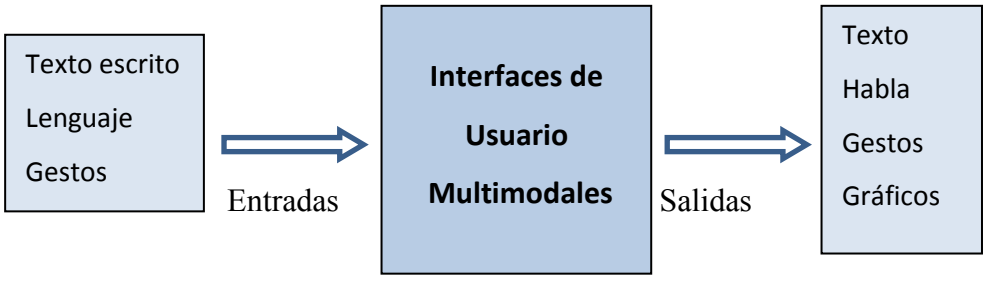

Figura 1.4. Esquema Interfaces Multimodales Inteligentes

Este es el principal motivo por el que resulta necesario seguir desarrollando nuevas formas de interacción que sean cada vez más naturales, de tal forma que la interacción del usuario con los dispositivos presentes en los dominios del AmI sea una interacción implícita, en la que no resulte necesaria la comunicación explícita del mismo con los

dispositivos de computación ubicua presentes en el entorno inteligente. Para lograr la naturalización de las interfaces de usuario multimodales, debe considerarse, tanto el conocimiento de los factores humanos, como la usabilidad, la accesibilidad y las metodologías tanto de diseño orientadas a metas y centradas en el usuario, como las de evaluación, de tal forma que los usuarios no necesiten ningún periférico específico para comunicarse del modo más adecuado, atendiendo a sus necesidades y/o circunstancias.

1.2.5.4. Consciencia del contexto

El sistema que se desarrolle en los entornos inteligentes del AmI ha de conocer ciertas cuestiones relacionadas con el entorno del usuario como son: ¿Dónde estamos? (Computación ubicua), ¿con quién estamos? (Comunicación ubicua), ¿cuáles son los servicios a los que tenemos acceso? (Interfaces multimodales), y por último ¿cómo se accede a estos servicios, y en qué modo se nos ofrecen? La respuesta a ésta última pregunta viene definida por el contexto en el que se encuentra el usuario, es decir, el conjunto de circunstancias relativas a su localización, entorno, identidad, y temporalidad. Dicho contexto nos dará información relativa a cuándo y cómo podemos acceder a determinados servicios que serán los más adecuados, según la situación en la que nos encontremos. De esta manera, el usuario no se verá saturado por una gran cantidad de servicios, sino que el sistema con consciencia del contexto desarrollado en AmI será capaz de ofrecérselos cuando pueda necesitarlos o solicitarlos.

El conocimiento de las diferentes acciones realizadas por los usuarios, pueden ser previstas analizando la situación en la que estos se encuentran *[Schilit, Adams & Want, 1994]*, de una forma similar al conocimiento de nuestra propia forma de comportarnos. Así, las aplicaciones con consciencia del contexto pueden dar lugar a distintas configuraciones y adaptaciones del sistema desarrollado en AmI, de tal forma que ante una misma petición por parte del usuario, el sistema sea capaz de ofrecer distintas respuestas según la información que tenga disponible del contexto.

No hay una definición de contexto y de sistemas con consciencia del contexto que se encuentre ampliamente aceptada. Algunas de las definiciones que aparecen más referenciadas y utilizadas en el ámbito de la computación son las que se citan a continuación:

Uno de los primeros trabajos que hacen referencia a la consciencia del contexto es el presentado por *[Schilit & Theimer, 1994]*, en el que los autores hablan de contexto en términos de *"ubicación, identidades de personas y objetos cercanos, así como de los cambios que sufren estos objetos"*. Por otra parte, en *[Ryan, Pascoe & Morse, 1997]* se define el contexto como *"la localización del usuario, el entorno, la identidad y el tiempo"*. Una de las definiciones más aceptadas es la propuesta por *[Anind K. Dey, 2001]*: *"Contexto es cualquier información que puede ser caracterizada para definir una situación de una entidad. Una entidad es una persona, lugar u objeto considerado relevante para la interacción entre un usuario y una aplicación, incluyendo al propio usuario y a la aplicación"*. De acuerdo con esta definición, el autor describe la computación consciente de contexto como un *"sistema que hace uso del contexto para proporcionar información relevante y/o servicios al usuario, donde la relevancia depende de la tarea del usuario".*

Atendiendo a estos conceptos y definiciones, podemos identificar cuáles son los elementos principales que conforman el contexto y que son: Usuario, Entorno, Servicio y Dispositivo.

- Usuario: individuo concreto con identidad propia
- Entorno: espacio que alberga objetos y personas
- Servicio: prestación que da el ambiente a personas o dispositivos
- Dispositivo: objetos del entorno que pueden prestar servicios conocidos en el sistema.

Teniendo en cuenta las diferentes acepciones del contexto, podemos decir que por su naturaleza se caracteriza por ser amplio, complejo y ambiguo. Por ello, es necesario establecer modelos que representen la realidad o, más concretamente, que representen el contexto como fuente de información.

Estos modelos de contexto han de definir los elementos relevantes al usuario, su entorno y situación, de forma que sea posible compartir esta percepción del mundo real, entre diferentes aplicaciones o sistemas *[Karen Henricksen, Indulska, & Rakotonirainy, 2002].*

Existen diferentes propuestas sobre cuáles son los aspectos fundamentales que ha de tener una aplicación para ser consciente del contexto; así por ejemplo en *[Schilit, Adams & Want, 1994]* los autores consideran que los aspectos más importantes son saber dónde se encuentra el usuario, con quién está y qué recursos existen alrededor. Estos autores consideran además que el espacio puede dividirse en varios entornos: entorno computacional (equipos informáticos, periféricos, etc.), entorno del usuario (ubicación, situación social, etc.) y entorno físico (iluminación, humedad, etc.). Debido a la naturaleza cambiante y dinámica que presenta el contexto, la mayoría de las dificultades con las que nos encontramos a la hora de desarrollar un sistema consciente del contexto, provienen de la adquisición no uniforme ni estandarizada de los datos del contexto, ya que éstos proceden de diversas fuentes a menudo heterogéneas, por lo que resulta necesaria la abstracción del mismo para su desarrollo *[Anind K. Dey, 2000]*.

Cualquier aplicación desarrollada en AmI con consciencia del contexto, ha de afrontar los problemas derivados de la captura de los datos del contexto, entre los que se encuentran: la imprecisión, la ambigüedad y los errores. Algunos investigadores plantean como solución a estos problemas involucrar al usuario, esto quiere decir que proponen el desarrollo de técnicas que utilicen la intervención del usuario y que son conocidas como técnicas de mediación *[Jeffrey Heer, et al. 2004]*, *[Anind K. Dey & J. Mankoff, 2005]*. Pero estas técnicas de mediación entran en conflicto con los objetivos de la Inteligencia Ambiental basados en la búsqueda de interacciones lo más naturales e implícitas posibles.

Por este motivo, el tratamiento de los problemas relacionados con la adquisición de los datos del contexto debe nutrirse del propio contexto y de las entradas implícitas del sistema, dejando las mínimas responsabilidades a la intervención del usuario. De esta forma, cuando el usuario rechace un determinado servicio ofrecido por el entorno, el sistema deberá recoger toda la información necesaria para evaluar esta situación solicitada por el usuario, de modo que convierta el rechazo del usuario en una entrada implícita, evitando así que vuelva a ofrecerse el servicio rechazado.

Así pues, definiendo un buen modelo de sistema con consciencia del contexto que sea capaz de aprender y de adaptarse a las particularidades de cada usuario, y con mecanismos que conviertan las acciones del usuario en fuentes de información (entrada implícitas), conseguiremos minimizar los problemas derivados de la adquisición de los datos del contexto, de una manera no intrusiva y sin interferir en las tareas que esté realizando el usuario. Las personas inmersas en un ambiente inteligente solo deben ser responsables de adecuar su perfil lo mejor posible para que los servicios ofrecidos por el sistema se adapten de forma proactiva a sus actividades y/o necesidades. Esta retroalimentación implícita es una estrategia de gran valor en la mayoría de las aplicaciones desarrolladas en Inteligencia Ambiental en las que, gracias a la consciencia del contexto, son capaces de razonar y adaptarse de forma eficaz al entorno que las rodea, ofreciendo así mejores servicios a los usuarios.

1.2.5.5. Implicaciones sociales y éticas

La visión de la Inteligencia Ambiental, como hemos visto, consiste fundamentalmente en la creación de entornos inteligentes en los cuales los usuarios interaccionan de una manera natural con diferentes servicios o aplicaciones, que se encuentran disponibles, en cualquier momento y lugar, a través de los diferentes dispositivos y tecnologías presentes en los dominios de aplicación del AmI. El acceso a estos servicios o aplicaciones tiene lugar a través de distintos modos de interacción socio-digital, en los cuales el entorno inteligente es capaz de obtener información personal del usuario y ofrecerle, así, un servicio personalizado y adaptado a sus preferencias o necesidades.

En este tipo de interacciones del usuario con los diferentes servicios o aplicaciones desarrollados en los dominios de aplicación del AmI, no solo es importante considerar los aspectos tecnológicos que caracterizan el entorno inteligente, sino que, además, deben tenerse en cuenta consideraciones sociales y éticas a la hora de diseñar y desarrollar las aplicaciones del AmI como son la seguridad, la fiabilidad y la privacidad.

Teniendo en cuenta que en la interacción y comunicación entre el usuario y el entorno inteligente, el entorno es capaz de obtener información personal del usuario al ofrecerle un servicio personalizado, resulta importante que esta información no solo sea fiable y segura, sino que se debe garantizar también la privacidad de la misma.

Los diferentes dispositivos y tecnologías presentes en los dominios de aplicación del AmI son capaces de adquirir, almacenar, gestionar y transmitir una gran cantidad de información y datos personales sobre los usuarios. Esto hace que el posible uso que pueda hacerse de los mismos, haya elevado de forma notable los riesgos a los que se enfrentan los usuarios desde el punto de vista social y ético, entre los que destacamos la privacidad como uno de los valores más importantes que hay que considerar en el diseño y desarrollo de las aplicaciones del AmI.

En la actualidad, los rápidos cambios tecnológicos y la globalización han hecho surgir nuevos retos y oportunidades para gobiernos y ciudadanos de todo el mundo, que han llevado a considerar el tema de la privacidad como un reto que va siendo cada vez más objeto de atención, sobresaliendo como un valor social fundamental. Resulta una idea generalizada en nuestra sociedad actual el hecho de considerar la necesidad de estandarizar y regular legalmente el acceso a la información del usuario, con el fin de evitar los problemas sociales y éticos mencionados *[F. Sadri, 2011]*.

Entre las razones más evidentes que nos llevan a considerar la necesidad de tener en cuenta las implicaciones sociales y éticas, y en especial, la protección de la privacidad en el diseño y desarrollo de las aplicaciones del AmI, podemos destacar las siguientes: la gran cantidad de información y datos personales que se obtienen del usuario, la persistencia en el tiempo de estos datos y su integración en diferentes lugares en los que son almacenados y gestionados, el control del flujo de estos datos,

tanto en el momento de enviarlos como en el momento en el que se comparten, y por último, el hecho de que cada vez es más fácil el acceso a la información personal de los usuarios en un mundo tecnológico que cada vez resulta más complejo.

Para que los sistemas desarrollados en Inteligencia Ambiental ofrezcan servicios de calidad, seguros y fiables para los usuarios, deben tenerse en cuenta no solo los factores técnicos a la hora de su diseño e implementación (computación y comunicación ubicua, interfaces inteligentes), sino que deben también considerarse los aspectos sociales y éticos, como la seguridad, la confianza y la privacidad.

Entre estas consideraciones sociales y éticas, destacamos la privacidad como una de las cuestiones de más relevancia para tener en cuenta en el diseño y desarrollo de las aplicaciones del AmI, ya que la privacidad constituye uno de los derechos fundamentales de las personas, como así queda reflejado en la Declaración Universal de los Derechos Humanos (Artículo 12), Convención Europea de los Derechos Humanos (Artículo 8), Acta Europea de los Derechos Humanos (Artículos 7 y 8), y en nuestra Constitución Española de 1978 (Artículo 18). El éxito y aceptación de las aplicaciones del AmI por parte de los usuarios depende en gran medida de cómo de seguras y fiables sean, y de cómo los usuarios las entiendan y sean conscientes de que se utilizan de una forma adecuada, y de que no ponen en riesgo su privacidad.

1.2.6. Potencial y ámbito de aplicación del AmI

La gran aspiración del paradigma de la Inteligencia Ambiental consiste en que las personas queden inmersas en un espacio o entorno digital (llamado entorno inteligente), que sea consciente de la presencia de las personas, sea sensible al contexto que las rodea, y que presente la capacidad de adaptarse a sus necesidades, hábitos y emociones *[ISTAG, 2001]*. Para lograr este objetivo, las tecnologías presentes en Inteligencia Ambiental han de ser capaces de interactuar con las personas de la manera más natural posible, en las diferentes actividades que realizan en su vida cotidiana al interaccionar con el entorno en el que se encuentran.

La Inteligencia Ambiental, más allá de su componente teórico tiene un claro objetivo práctico, ya que su principal finalidad se basa en desarrollar aplicaciones reales y eficaces que puedan ser utilizadas por las personas, de la manera más natural y fácil posible, ayudando así a la realización de las diferentes tareas que realizamos a diario; por ello resulta necesario desarrollar nuevas herramientas y métodos de investigación, que nos permitan tener un mayor conocimiento de los requerimientos reales que se necesitan en el diseño y desarrollo de las aplicaciones del AmI *[Ruyter B. & E. Aarts, 2004]*.

Podemos entender la Inteligencia Ambiental como un abanico que abarca no solo áreas tecnológicas como la Computación Ubicua *[Mark Weiser, 1993]*, las Interfaces Naturales *[Coen, M. 1998]* y las Comunicaciones Ubicuas *[G. Chen & Kotz, 2000]*, sino que en ella se encuentran englobadas diferentes áreas de investigación relacionadas con cuestiones sociales y éticas. Así pues, la Inteligencia Ambiental es un campo de investigación multidisciplinar que incorpora diversas tecnologías procedentes de una gran variedad de disciplinas: Electrónica, Domótica, Automatización, Redes de sensores inalámbricos, Sistemas de monitorización, Sensores inteligentes, Redes de Comunicaciones, Interfaces multimodales Inteligentes, Agentes Inteligentes, Visión artificial, etc. Por ello, resulta un aspecto clave a la hora de desarrollar los entornos inteligentes presentes en las aplicaciones del AmI, integrar todas estas tecnologías, para que el entorno inteligente sea capaz de aprovechar las ventajas que presenta cada tecnología, y ofrezca al usuario un conjunto de servicios útiles, sencillos de manejar, personalizados según sus necesidades y preferencias, y a la vez, que resulten seguros y de confianza para el usuario y no pongan en riesgo su derecho a la privacidad.

Los usos potenciales que presentan las aplicaciones del AmI son tan amplios que incluso se ha financiado un proyecto para construir, desde cero, ciudades que incorporen las tecnologías más novedosas para crear ciudades ubicuas. Uno de los casos más ambiciosos es "New Songdo City", la metrópoli futurista del siglo XXI *[http://www.songdo.com]*. Se trata de un ambicioso proyecto de creación de una ciudad ubicua en la que todos los sistemas de información de viviendas, negocios, organismos oficiales, etc. se encuentran interconectados, para que todo pueda interactuar a través de estos sistemas de información comunicados mediante tecnologías como las redes inalámbricas o RFID. Esta "Smart City" se encuentra situada en una isla artificial frente a la ciudad de Incheon, a 60 Km al oeste de Seúl (Corea del Sur), en una superficie de 680 hectáreas. Se estima que la duración del proyecto sea de 10 años y que costará más de 40 mil millones de dólares.

En todas las construcciones que se realicen en esta ciudad se integrarán todas las tecnologías necesarias para facilitar el acceso, uso y disfrute de las mismas por parte de los ciudadanos, proporcionándoles de esta forma una mayor calidad de vida. Como ejemplos tenemos los siguientes: las papeleras de la ciudad estarán provistas de sensores y etiquetas RFID para saber si están llenas y proceder de esta manera a su recogida y limpieza, además de abonar una cantidad en la cuenta bancaria del usuario que recicle botellas vacías; la existencia de sensores de movimiento en los domicilios de las personas mayores que detectan posibles caídas o golpes, y poder avisar de forma automática a los servicios de ayuda o ambulancias.

Los ciudadanos de New Songdo City dispondrán de una tarjeta inteligente que les servirá para realizar la mayoría de las actividades diarias, como utilizar el metro, pagar en los parkings, comprar entradas para el cine, abrir la puerta de sus viviendas, etc. A finales del año 2015, todos los sistemas de información presentes en la ciudad (residenciales, médicos, negocios y comercios) estarán interconectados e integrados en las viviendas, las calles y los edificios de oficinas.

El ámbito de aplicación de la Inteligencia Ambiental es muy extenso, y abarca campos muy diversos en los que realizamos la mayoría de nuestras actividades cotidianas. En la actualidad, la mayoría de las aplicaciones desarrolladas en AmI se encuentran focalizadas en las siguientes áreas o dominios: los entornos domésticos, el cuidado de la salud y las tecnologías de asistencia (Ambient Assisted Living, AAL), la educación, los negocios, el comercio, el transporte, el ocio, el turismo, etc.

El dominio de aplicación de las tecnologías del AmI en nuestra vida cotidiana es tan amplio y se encuentra tan extendido en la actualidad, que las diferentes interacciones entre ellas y las que se producen con los usuarios conforman un nuevo escenario de convivencia en el que resulta necesario tener en consideración tanto la adaptabilidad y mejora de los sistemas a nivel tecnológico, como su evolución a nivel social.

Capítulo 2

Motivación y Objetivos

2.1. MOTIVACIÓN

Teniendo en cuenta las capacidades y características que deben tener los entornos inteligentes desarrollados en Inteligencia Ambiental descritos en el capítulo anterior como son: sensibilidad al contexto, encontrarse inmersos en el ambiente, tener capacidad de computación y comunicación, ser operativos mediante interacciones naturales, y considerando los fundamentos sobre los que debe asentarse el desarrollo de las aplicaciones del AmI en las que tienen lugar distintos tipos de interacción socio-digital entre el entorno inteligente y los usuarios, resulta fundamental tener en consideración las implicaciones sociales y éticas para el verdadero desarrollo y aceptación de la Inteligencia Ambiental por parte de los usuarios.

Casi todas las actividades que realizamos a diario a través de las tecnologías presentes en Inteligencia Ambiental hacen que cada vez resulte más fácil la adquisición de información y datos personales de los usuarios, el control o monitorización de su comportamiento, así como la transmisión de su información personal a terceros, sin que el usuario sea consciente y haya dado su consentimiento en la mayoría de las ocasiones. El gran volumen de datos que son adquiridos y gestionados a través de las aplicaciones desarrolladas en AmI, así como su persistencia, han elevado de manera notable los riesgos de privacidad de los usuarios, y el uso de los mismos está siendo utilizado de maneras que no habían sido previstas en el momento en el que habían sido adquiridos, pudiendo ofrecer conocimientos intrínsecos de los individuos respecto a sus intereses, preocupaciones, actividades, costumbres, salud, orientación sexual, ideas políticas, etc., que ponen en riesgo nuestra privacidad.

Este aumento de los riesgos de privacidad señala la necesidad de establecer garantías más eficaces que ayuden a la protección de la privacidad de nuestra información personal, a la hora de acceder a los diferentes servicios ofrecidos por las aplicaciones desarrolladas en Inteligencia Ambiental.

Cualquier dispositivo o tecnología con el que interactúe el usuario, ya sea con o sin su conocimiento sobre la existencia del mismo, debería notificar al usuario de su capacidad para adquirir información personal sobre él, así como de su capacidad para almacenarla, gestionarla, compartirla, etc. con otros dispositivos o aplicaciones que pueden ser desconocidos para el usuario.

En la actualidad, ya no nos resulta extraño el hecho de que al pasar delante de un determinado establecimiento, como puede ser un restaurante en el que en algún momento hemos contactado a través de las aplicaciones de Internet con nuestro Smartphone, recibamos un mensaje en nuestro teléfono móvil en el que se nos muestre el menú del día, sin que lo hayamos solicitado o hayamos dado nuestro consentimiento para ello.

La tecnología y dispositivos presentes en los dominios de aplicación de la Inteligencia Ambiental deben servir no solo para facilitar y dar soporte a las diferentes actividades cotidianas que realizamos, sino que deben también ser utilizados para ayudar a preservar la privacidad de nuestros datos e información personal. El nivel de conocimiento general que tienen los usuarios acerca de las políticas de privacidad y de cómo se gestionan al acceder a los servicios desarrollados en Inteligencia Ambiental es bastante reducido, hecho que se acentúa notablemente si consideramos algunos dominios de aplicación como es el del Ambient Assisted Living, en el que los usuarios son especialmente vulnerables frente al problema de la privacidad.

La mayoría de los estudios realizados sobre las aplicaciones del AmI están enfocados a las tecnologías utilizadas (dispositivos computacionales y dispositivos de comunicación), en algunos casos a la usabilidad por parte de los usuarios, y en pocos casos tienen en cuenta las cuestiones sociales y el impacto de la privacidad que supone el uso de las mismas.

Como hemos visto, uno de los principales elementos que se debe tener en cuenta en el desarrollo de las aplicaciones del AmI, cuyo objetivo es el de facilitar y dar soporte a las diferentes actividades desarrolladas en los entornos inteligentes es el usuario, por este motivo deben ser las aplicaciones y servicios ofrecidos en AmI los que tengan en cuenta las implicaciones sociales y éticas de los usuarios.

El modo en el que se diseñe e implemente las cuestiones sociales y éticas, y en concreto el tema de la privacidad en las aplicaciones desarrolladas en Inteligencia Ambiental, resulta esencial para que el usuario confíe en los servicios ofrecidos por el AmI. La interacción entre los entornos inteligentes y los usuarios debe ser transparente, y no invisible, el usuario ha de saber qué tecnologías están presentes cuando accede a los servicios ofrecidos por el AmI. De esta forma, los servicios ofrecidos por las aplicaciones del AmI, no solo darán soporte y mejorarán la realización de nuestras actividades cotidianas de una forma más accesible, cómoda, y personalizada, sino que también servirán para incrementar nuestro grado de confianza, ofreciéndonos garantías sobre la protección de nuestro derecho a la privacidad.

Cuando confiamos en alguien, compartimos nuestros asuntos íntimos porque sabemos que están a salvo, confiar en los servicios ofrecidos por las tecnologías utilizadas en las aplicaciones desarrolladas en Inteligencia Ambiental implica saber que dichas tecnologías nos ayudan a proteger nuestra privacidad.

2.2. HIPÓTESIS Y OBJETIVO

Considerando que la confianza en la transmisión de nuestra información personal puede servirnos para minimizar los riesgos de privacidad de la misma, se plantea la hipótesis de trabajo de la memoria que consiste en la utilidad de los Sistemas Multiagente (MAS) en los modelos de confianza, como herramienta que nos ayude a minimizar los riesgos de privacidad de nuestra información personal considerando un determinado dominio de aplicación de la Inteligencia Ambiental.

El objetivo propuesto de esta tesis es el de presentar un Modelo de Privacidad Digital basado en Sistemas Multiagente que, teniendo en cuenta diferentes políticas de privacidad, nos ayude a decidir en quién podemos confiar a la hora de compartir nuestras opiniones privadas utilizando el entorno de experimentación del ART testbed (Agent Reputation and Trust) en el dominio relacionado con la tasación de cuadros de arte.

Para la validación de este modelo se establecerán las decisiones que deben tomar los agentes en sus comunicaciones, que serán las que nos ayuden a decidir cuáles son los agentes de confianza con los que compartir nuestras opiniones privadas.

Para llegar a alcanzar este objetivo, se plantea la realización de los siguientes objetivos específicos:

- Revisar las aplicaciones desarrolladas en Inteligencia Ambiental.
- Realizar una clasificación de los principales dominios de aplicación del AmI.
- Realizar una clasificación de las principales tecnologías utilizadas en AmI.
- Definir los aspectos socio-tecnológicos más relevantes de las aplicaciones del AmI.
- Presentar el marco legal del derecho a la privacidad.
- Estudiar la privacidad en Inteligencia Ambiental: modelos de privacidad.
- Definir el marco conceptual de privacidad en AmI “Design by Privacy”.
- Definir las políticas de privacidad en el diseño de las aplicaciones del AmI.
- Evaluar el grado de protección requerido de la información personal en base al dominio de aplicación del AmI.
- Establecer los niveles de protección de la información.
- Determinar los derechos de privacidad que deben cumplir los agentes de nuestro modelo de confianza en sus comunicaciones.
- Implementar los mensajes adicionales de los agentes en los protocolos de las relaciones de confianza del entorno de experimentación ART tetbed, para cumplir con los derechos de privacidad.

- Formalizar los protocolos de comunicación de los agentes siguiendo el estándar FIPA (Foundation for Intelligent Physical Agents).
- Validar la manera de decidir con quién compartimos nuestras opiniones privadas.

2.3. METODOLOGÍA DE LA INVESTIGACIÓN

En primer lugar se realizó una introducción sobre el área de investigación del trabajo presentado, la Inteligencia Ambiental, en la que se presentaron las capacidades y las principales características que conforman los sistemas desarrollados en AmI y que sirvieron para establecer los fundamentos sobre los que debe asentarse la Inteligencia Ambiental en el desarrollo de sus aplicaciones: los dispositivos de computación ubicua, las comunicaciones ubicuas, las interfaces de usuario inteligentes, la consciencia del contexto y las implicaciones sociales y éticas.

Esta introducción sirvió para entender la Inteligencia Ambiental como un amplio abanico multidisciplinar en el que se encuentran englobadas diversas áreas de investigación relacionadas con diferentes tecnologías de computación y comunicación, así como las relacionadas con cuestiones de tipo social y ético.

A partir de estas consideraciones, se llevó a cabo un estudio sobre las aplicaciones desarrolladas en Inteligencia Ambiental, con el objetivo de determinar los principales dominios de aplicación del AmI y las principales tecnologías utilizadas. Tras este estudio se extrajeron conclusiones sobre la importancia de tener en cuenta las cuestiones de tipo social y ético en el desarrollo de las aplicaciones del AmI, destacando el tema de privacidad como uno de los principales retos que debe abordarse para mejorar y potenciar los servicios ofrecidos por las aplicaciones desarrolladas en AmI.

A continuación, la investigación se focalizó en el estudio de la privacidad, presentándose el marco legal del derecho a la misma, así como los diferentes modelos de privacidad propuestos en Inteligencia Ambiental.

Teniendo en cuenta el concepto "Design by Privacy" se establece un marco conceptual de privacidad en AmI, en el que se tienen en cuenta diferentes políticas de privacidad y que han servido para determinar el nivel de protección de los datos e información del usuario en los principales dominios de aplicación del AmI.

A partir de las políticas establecidas en el modelo conceptual "Design by Privacy" y habiendo establecido los diferentes niveles de protección de la información (cumpliendo con la normativa legal UE, 2016/679) se determinan los derechos de privacidad que deben cumplir los agentes del modelo de confianza propuesto en sus comunicaciones.

Para establecer la protección de la privacidad de la comunicación entre los agentes de nuestro modelo de confianza, se llevó a cabo la integración de estos derechos estableciendo una serie de mensajes adicionales en los protocolos de comunicación de las relaciones de confianza del entorno de experimentación ART testbed. Estos mensajes se formalizaron siguiendo el estándar FIPA (Foundation for Intelligent Physical Agents) utilizando la plataforma del ART testbed implementada en el entorno de JADE.

A continuación se valida la propuesta utilizando los datos de la competición del ART testbed de 2007, en la que se comparan las opiniones de tres agentes sobre una colección de 57 cuadros con la estimación final de los mismos. Para ello, se define la manera en la decidimos quiénes son los agentes de confianza con los que vamos a compartir nuestras opiniones privadas, utilizando como herramienta de aprendizaje automático WEKA.

Con esta herramienta se establecen unos atributos de entrada (valores de las opiniones de los agentes) y un atributo como salida (nuestra variable objetivo) que nos servirá para determinar cuáles son los agentes en los que vamos a confiar para compartir con ellos nuestras opiniones privadas, que serán los agentes cuyo valor se aproxime más al valor de la estimación final, y que define nuestra variable objetivo.

Para terminar y con el fin de controlar el cumplimiento de los derechos de privacidad establecidos, se definen las posibles infracciones de privacidad que pueden tener lugar en las comunicaciones entre los agentes, y que se han formalizado a través de la Institución Electrónica "Islander" utilizada como herramienta de especificación de las normas y sanciones correspondientes que deben cumplir los agentes en sus comunicaciones.

2.4. ESTRUCTURA DE LA MEMORIA

La memoria presentada, se encuentra dividida en cuatro partes: Introducción; Estado del arte; Propuesta, Desarrollo y Caso de estudio; y, para finalizar Conclusiones y Trabajo futuro.

La primera parte (Parte I. Introducción), se compone de dos capítulos: Capítulo 1 "Introducción", y Capítulo 2 "Motivación y Objetivos". La segunda parte (Parte II. Estado del arte), se desarrolla en dos capítulos: Capítulo 3 "Aplicaciones del AmI", y Capítulo 4 "La privacidad en AmI". La tercera parte de la memoria (Parte III. Propuesta, Desarrollo y Caso de estudio), consta del Capítulo 5 "Marco Conceptual de Privacidad en AmI", y del Capítulo 6 "Modelo de Privacidad Digital en AmI basado en Sistemas Multiagente". La última parte (Parte IV. Conclusiones y Trabajo futuro), contiene el Capítulo 7 "Conclusiones y Trabajo futuro". Para finalizar, se incluyen las referencias bibliográficas citadas en la memoria presentada (y que aparecen indicadas por orden de aparición). Se incluye también al final del Índice General de la memoria, el Índice de Figuras y el Índice de Tablas.

A continuación, se presenta un resumen de los capítulos que componen el trabajo de investigación realizado:

- *Capítulo 1 "Introducción"*. En este capítulo se expone el marco sobre el que se ha desarrollado la tesis, la Inteligencia Ambiental, identificándose las características y los fundamentos que conforman el área de investigación del AmI, así como el potencial y ámbito de aplicación del mismo.

- *Capítulo 2 "Motivación y Objetivos"*. A partir de las consideraciones realizadas en la Introducción, en este capítulo se identifica el problema que ha motivado el trabajo de investigación realizado, se plantea la hipótesis de trabajo y el objetivo de la investigación realizada, indicándose la metodología llevada a cabo para la realización de la misma.

- *Capítulo 3 "Aplicaciones del AmI"*. Este capítulo se centra en el estado del arte de las aplicaciones desarrolladas en Inteligencia Ambiental. Se presenta la evolución de la Inteligencia Ambiental y los entornos inteligentes, y se realiza una revisión de las principales aplicaciones desarrolladas en AmI. A partir de este estudio se lleva a cabo una clasificación de los principales dominios de aplicación del AmI, y de las principales tecnologías utilizadas en el desarrollo de dichas aplicaciones. A continuación se presentan distintos tipos de aplicaciones desarrolladas en AmI atendiendo a esta clasificación. Finaliza el capítulo con unas conclusiones acerca del gran número de investigaciones sobre las aplicaciones del AmI realizadas en los últimos 15 años, que ha permitido establecer la importancia de considerar los aspectos socio-tecnológicos. Entre estos aspectos destaca la privacidad, como uno de los principales retos a abordar que servirá para mejorar la confianza de los servicios ofrecidos por las aplicaciones desarrolladas en Inteligencia Ambiental.

- *Capítulo 4 "La privacidad en AmI"*. En este capítulo se define el concepto de privacidad y se establece el marco legal que regula el derecho a la misma. Se presentan los aspectos relacionados con la privacidad que hay que tener en cuenta en el desarrollo de las aplicaciones del AmI, se exponen los modelos de privacidad propuestos en Inteligencia Ambiental y, se establece la necesidad de establecer garantías de la privacidad de la información de los usuarios a partir del establecimiento de diferentes políticas de privacidad. Se termina indicando la estrecha relación entre los conceptos de confianza y privacidad, que pueden ser consideradas de manera conjunta para ayudarnos a proteger nuestra información personal en los dominios de aplicación del AmI.

- *Capítulo 5 "Marco conceptual de privacidad en AmI"*. A partir del estado del arte de las aplicaciones del AmI, en este capítulo se presentan los principales aspectos que deben tenerse en el diseño del AmI, y que han servido para establecer las políticas de privacidad del modelo conceptual "Design by Privacy" en AmI. Este modelo ha servido para determinar el nivel de protección de los datos e información de los usuarios según el dominio de aplicación del AmI.

- *Capítulo 6 "Modelo de Privacidad Digital en AmI basado en Sistemas Multiagente"*. A partir de los niveles de protección de los datos que deben cumplir los modelos de confianza, en este capítulo se establecen los mensajes que deben intercambiar los agentes en sus comunicaciones para cumplir con los derechos de privacidad que han sido establecidos de acuerdo a la normativa legal (Regulation EU, 2016/679). Estos mensajes (protocolos) se implementan utilizando el entorno de experimentación del ART testbed (en el que los agentes participantes actúan como tasadores de cuadros de arte) dando así cumplimiento a los derechos de privacidad establecidos.

Una vez aplicados estos mensajes se valida el modelo estableciendo la manera en la que vamos a decidir cuáles son los agentes en los que vamos a confiar para compartir con ellos nuestras opiniones privadas, utilizando para ello la competición del ART testbed de 2007 y la herramienta de aprendizaje automático WEKA (v.3.6.1.). Se presentan los resultados obtenidos que nos muestran el porcentaje de aciertos por clasificador para decidir el agente en el que confiamos. Finaliza el capítulo con la formalización a través de la Institución Electrónica "Islander" de las posibles infracciones de los derechos de privacidad que pueden cometer los agentes en sus comunicaciones.

- *Capítulo 7 "Conclusiones y Trabajo futuro"*. Este capítulo resume las conclusiones obtenidas del trabajo de investigación realizado y, las posibles líneas de investigación futuras. Para terminar, se detalla la producción científica, publicaciones y participación en proyectos I+D+i, que ha dado como resultado el trabajo de investigación de esta tesis.

PARTE II

ESTADO DEL ARTE

Capítulo 3

Aplicaciones del AmI

3.1. INTRODUCCIÓN

El ámbito de aplicación de la Inteligencia Ambiental es muy extenso y abarca campos muy diversos en los que realizamos la mayoría de nuestras actividades cotidianas. El ámbito de aplicación del AmI incluye múltiples y diversas áreas de nuestra vida, como son los entornos domésticos, la oficina, la salud y las tecnologías de asistencia (Ambient Assisted Living, AAL), el transporte, la industria, la educación, los negocios, el comercio, el ocio, el turismo, los sistemas de recomendación, la seguridad, etc.

La gran aspiración del paradigma de la Inteligencia Ambiental consiste en que las personas queden inmersas en un espacio o entorno digital (llamado entorno inteligente), que es consciente de la presencia de las personas, sensible al contexto en el que se encuentran, y que además, presenta la capacidad de adaptarse a sus necesidades, hábitos y emociones *[ISTAG, 2001-2002]*. Para lograr este objetivo, las tecnologías presentes en los dominios de aplicación de la Inteligencia Ambiental han de ser capaces de interactuar con las personas, de la manera lo más natural posible, en las diferentes actividades que realizan en su vida cotidiana.

3.2. EVOLUCIÓN DEL AmI Y ENTORNOS INTELIGENTES

En los Entornos o Ambientes Inteligentes (Intelligent Environment, IE) provistos de dispositivos de detección y computación ubicua, los sistemas basados en la adquisición de consciencia del contexto son una de las soluciones más idóneas para el desarrollo de las aplicaciones del AmI. La computación con consciencia del contexto (Context Aware Computing), puede definirse como la capacidad que presentan los dispositivos de computación para detectar y conocer, e interpretar y responder a aspectos relacionados con el entorno que rodea al usuario y con los propios dispositivos que conforman el sistema *[Hull, R. et al. 1997]*.

Así pues, un sistema se considera con consciencia del contexto, si utiliza el contexto en el que se encuentra para proporcionar información relevante y/o servicios al usuario que dependan de la tarea que el usuario esté realizando *[Dey, AK. and Abowd, GD. 1999]*.

Los sistemas desarrollados en Inteligencia Ambiental representan una nueva generación de sistemas *[Weber, W. et al. 2005]* que presentan las siguientes características:

- Invisibles: se pueden encontrar embebidos en ropa, relojes, pulseras, etc.
- Móviles: pueden ser transportados y usarse en diferentes sitios.
- Presentan consciencia del contexto: obtienen información del entorno en el que se encuentran (local), pudiendo extrapolarla a sitios similares de su periferia (vecindad).
- Anticipativos: actúan en su propio nombre sin necesidad de ninguna respuesta explícita por parte del usuario.
- Comunicación de forma natural: voz, gestos, imágenes.
- Adaptativos: capaces de reaccionar en toda clase de situaciones excepcionales y de una manera flexible sin la interrupción del servicio prestado.

Estos sistemas creados en los Entornos Inteligentes del AmI permiten a los usuarios interactuar con los servicios de computación ofrecidos por el sistema, de un modo natural e intuitivo, facilitándoles la realización de diversas tareas en distintos ámbitos de su vida cotidiana, como son el entorno doméstico, laboral, ocio, etc. *[Weiser, M. 1991], [Aarts, E. Manzano, 2003].* El procesamiento más significativo de la información, realizado por los dispositivos de detección y computación, se lleva a cabo principalmente a través de los sensores, por lo que resulta fundamental que en el desarrollo de las aplicaciones en estos Entornos Inteligentes del AmI, se tengan en consideración las posibles modificaciones en el número y/o clase de los sensores y dispositivos computacionales, en las fuentes de detección, así como en su modelado.

En la actualidad, la incorporación de nuevas formas de interacción de las personas como el habla y los gestos en los Entornos Inteligentes desarrollados en AmI, no solo ofrece mejoras en la adquisición y distribución de la información del contexto, sino que también permite a los usuarios acceder de una manera fácil y cómoda a los servicios ofrecidos por el AmI, en la que no resulta necesario encontrarse cerca de los dispositivos que integran el sistema *[Nieuwoudt, C. and Both, EC. 2002]*, *[Rebman, CMJ. et al. 2002]*.

El desarrollo de la Inteligencia Ambiental nos permite estar rodeados de Entornos Inteligentes en los que se encuentran inmersos múltiples y diversos dispositivos de computación y comunicación que son capaces de adquirir, almacenar, gestionar y transmitir diferentes tipos de información, gracias a la utilización de diferentes tecnologías computacionales.

Además gracias a las diferentes redes de sensores inalámbricos (WSN, Wireless Sensor Network) que se encuentran presentes en la mayoría de los dominios de aplicación del AmI, se facilita la comunicación entre los diferentes dispositivos, y entre éstos y el usuario *[Reynolds, F. et al. 2006]*.

Teniendo en cuenta el importante desarrollo de los Entornos Inteligentes del AmI en los últimos años, se presenta a continuación una actualización del gráfico que representa la evolución del AmI *[Jean Baptiste, 2007]:*

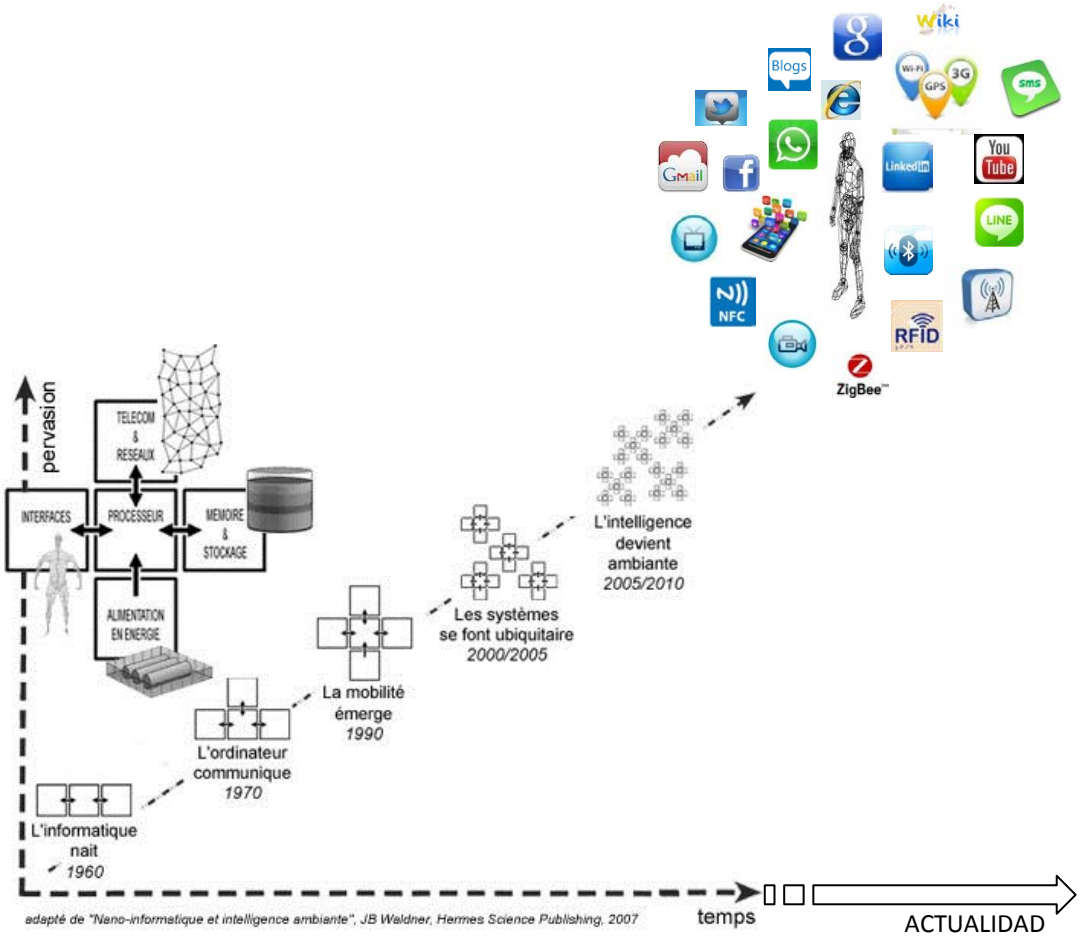

Figura 3.1. Evolución del AmI (Basada en la Evolución de la Informática "Nano-informatique et intelligence ambiente", Jean Baptiste Waldner, Hermes Science Publishing, 2007)

El uso de las Tecnologías de la Información y la Comunicación en el desarrollo de los Entornos Inteligentes del AmI ha tenido un gran impacto en los últimos 10 años, lo cual ha permitido que los dispositivos y tecnologías presentes en estos entornos se encuentren embebidos en muchos de los objetos cotidianos que rodean al usuario, y en el propio usuario también. Todo esto ha llevado a la creación de entornos digitales capaces de adaptarse de manera inteligente al contexto en el que se encuentra el usuario, anticiparse a sus necesidades, aprender de su comportamiento, y llegar incluso a tener la capacidad de reconocer, expresar y responder a las emociones.

Considerando la visión de futuro de la Inteligencia Ambiental en la que el entorno que nos rodea es sensible a nuestras necesidades o requerimientos, y cuya interacción tiene lugar de una manera fácil, anticipatoria, adaptable, dinámica, embebida, e inteligente, podemos establecer las principales capacidades que deben tener los sistemas que conforman los Entornos Inteligentes en el desarrollo de la Inteligencia Ambiental:

- Capturar toda la información asociada al usuario y al contexto en el que se encuentra, incluyendo las experiencias y tareas realizadas por el usuario en el desarrollo de su actividad cotidiana con los servicios ofrecidos por el entorno.

- Acceder tanto a la información propia del sistema como a nueva información que puede obtenerse del exterior, como puede ser a través de Internet. El acceso a esta información debe ser posible de diferentes modos y desde cualquier lugar de una manera eficiente.

- Dar soporte a la colaboración y a la comunicación. Los sistemas desarrollados en los Entornos Inteligentes del AmI, deben ofrecer capacidades de comunicación que puedan establecerse en cualquier lugar, y que requieran el menor esfuerzo posible por parte de los usuarios; es decir, la implementación de los mismos debe ser extensible a todos los escenarios con los que interactúe el usuario, interconectando los diferentes sistemas integrantes de forma eficiente.

- Desarrollar entornos sensibles al contexto (con consciencia del contexto). Los Entornos Inteligentes deben ser sensibles tanto a la información del entorno, como a la información del usuario. Para ello, el sistema debe disponer de herramientas que sean capaces de adquirir dicha información, procesarla, y en función de los resultados del análisis de la misma, ofrecer los servicios solicitados y/o modificar su comportamiento.

- Actuar como un guía automático; es decir, el sistema debe ser capaz de detectar a los usuarios y en función de su perfil, adaptarse y anticiparse a sus necesidades o peticiones, facilitándoles así los servicios de información requeridos, guiándoles en el entorno en el que se encuentren.

- Proporcionar nuevas formas de interacción entre el usuario y los sistemas de computación. El sistema debe disponer de una amplia variedad de interfaces de usuario que le permitan a éste interactuar con el entorno que le rodea. Estos interfaces deben ser lo más naturales, ubicuos y transparentes como sea posible, y ser multimodales para adaptarse a la diversidad de entornos con los que convive el usuario, y a la gran heterogeneidad de los dispositivos que interaccionan con el sistema.

- Considerar los aspectos sociales y éticos relativos a los datos e información que el sistema es capaz de adquirir, almacenar, gestionar y transmitir, poniendo en riesgo la protección de la privacidad de los usuarios.

3.3. REVISIÓN DE LAS APLICACIONES DEL AmI

En el desarrollo de las aplicaciones del AmI, convergen distintas áreas de la computación entre las que destacan: la computación ubicua, la comunicación ubicua y la inteligencia artificial. Las tecnologías de computación y comunicación ubicua, junto con los interfaces inteligentes (multimodales, visuales, sonoros, hablados), la inteligencia artificial y los sistemas multiagente, se han visto mejorados con la incorporación de las redes de sensores, los rastreadores de movimiento y localización, los sistemas de apoyo a la toma de decisiones, las comunicaciones móviles y las redes inalámbricas. Todo ello ha permitido un avance considerable en los servicios ofrecidos por el AmI.

Los dominios de aplicación del AmI se encuentran muy extendidos en la mayoría de nuestras actividades cotidianas, gracias a los avances en el desarrollo de las tecnologías inalámbricas, las redes de sensores, las capacidades de los display, la velocidad de procesamiento de la información, los servicios móviles, los interfaces multimodales, etc.

En el estudio presentado en *[Ubiquitous computing: Towards understanding European Strengths and Weaknesses, 2000],* se muestra la fortaleza y las debilidades detectadas en el desarrollo de la Inteligencia Ambiental en Europa. La siguiente tabla, presenta las posiciones de las capacidades desarrolladas en AmI tanto desde el punto de vista científico-tecnológico, como desde el punto de vista de la industria y el comercio:

Key Enabling Technology	**Position of Europe**				
	strong		*Medium*		*weak*
(1) embedded intelligence			■		
virtual & interactive reality			■		
intelligent identifiers, autonomously communicating objects		■			
real time transmission of multimedia contents		■	■		
software engineering & components			■		
intelligent homes			■		
(2) middle-ware & distributed systems			■		
big server networks			■		
integration of appliances, XML & other evolved languages		■			
(3) IP mobile & wireless	■				
portable digital assistants	■				
(4) multi-domain network management			■		
quality of IP service			■		
(5) converging core and access networks		■			
high transit backbone networks		■			
(6) micro- and opto-electronics			■		
silicon micro-electronics	■	■			
optic-electronic & photo-components	■	■			
search engines & intelligent indexing			■		
micro-electronics III V			■		
batteries, micro-energy			■		
mass memories					■
flat screens				■	■
(7) trust and confidence enabling tools			■		■
(8) cross media content					■
authoring systems for creating multimedia contents					■
(9) multi-modal and adaptive interfaces			■		
virtual & interactive reality			■		
(10) multi-lingual dialogue mode	■				
linguistic & vocal technologies	■				
Legend	■	scientific & technical position industrial & commercial position			

Tabla 3.1. Adapted from: Rapport Technologies.Clés 2005.
(Ministère de l'economie et de l'industrie. Paris, 2000)

Una vez realizado el estudio sobre las aplicaciones desarrolladas en Inteligencia Ambiental, hemos establecido una clasificación de los principales dominios o ámbitos de aplicación del AmI, en los cuales se han identificado las principales tecnologías involucradas en el desarrollo de dichas aplicaciones. Los principales dominios de aplicación del AmI que han sido establecidos se dividen en cuatro grandes áreas:

- Smart Home/ Salud/Tecnologías de Asistencia (AAL, Ambient Assisted Living)
- Educación
- Comercio y Negocios/Servicios Públicos y Transporte/ Sistemas de Recomendación
- Ocio y Entretenimiento

Las principales tecnologías utilizadas en el desarrollo de las aplicaciones del AmI estudiadas, han sido agrupadas en las siguientes categorías:

- Sensores inteligentes
- Redes de comunicación inalámbricas
- Interfaces de usuario multimodales
- Plataformas inteligentes

		Tecnologías del AmI
Dominios de Aplicación del AmI	Smart Home Salud Tecnologías de Asistencia (AAL)	Sensores inteligentes Redes de comunicación inalámbricas Interfaces de usuario multimodales Plataformas inteligentes
	Educación	
	Comercio y Negocios Servicios Públicos y Transporte Sistemas de Recomendación	
	Ocio y Entretenimiento	

Figura 3.2. Dominios y Tecnologías de las Aplicaciones del AmI

3.4. PRINCIPALES DOMINIOS DE APLICACIÓN DEL AmI

A continuación se presentan algunas de las aplicaciones estudiadas, desarrolladas en Inteligencia Ambiental, que han sido agrupadas según los dominios de aplicación que hemos establecido: Smart Home/Salud/Tecnologías de Asistencia; Educación; Comercio y Negocios/Servicios Públicos y Transporte/Sistemas de Recomendación; y por último Ocio y Entretenimiento.

3.4.1. Smart Home/ Salud/Tecnologías de Asistencia (AAL)

El concepto de Smart Home es el de una casa equipada con sensores, activadores (para el control de los sensores), y dispositivos computacionales (pequeños electrodomésticos) de diferentes tipos, que sirven para monitorizar la actividad y movimiento dentro del hogar, así como el riesgo de que ocurran determinadas situaciones de peligro (humo, fuego, caídas, etc.). La monitorización de las actividades que realizan los habitantes de la casa y su comparación con el perfil de los mismos, permite llevar a cabo las acciones necesarias en cada situación, proporcionando así la ayuda necesaria para el cuidado de la seguridad, salud y medicación, así como para otras actividades relacionadas con el ocio y el entretenimiento.

La mayoría de las aplicaciones desarrolladas en el dominio del entorno doméstico tienen como objetivo ayudar a un amplio colectivo formado por personas mayores, personas con algún tipo de enfermedad, o con algún tipo de discapacidad, en las diferentes actividades que realizan a diario, proporcionándoles mejor calidad de vida y mayor grado de independencia (Ambient Assisted Living, AAL).

Los servicios ofrecidos por las aplicaciones del AmI en el entorno doméstico incluyen:

- Realización de diferentes tareas cotidianas de forma automática.
- Mejora del factor económico en el uso de determinados servicios como la electricidad.

- Mejora de la seguridad y protección, previniendo accidentes.
- Mejora de la calidad de vida, ofreciendo diferentes grados de confort.
- Apoyo a la vida independiente de personas mayores y personas discapacitadas.

En el trabajo presentado por *[Friedewald, M. et al. 2005]* se analizan las posibilidades que puede ofrecer el AmI en un entorno doméstico, entre las que destacan cuatro áreas fundamentales: Domótica (control de la electricidad, calefacción, aire acondicionado, alarmas de fuego e intrusión), Comunicación y Socialización (Internet, dispositivos portátiles o manos libres), Descanso/Innovación/Deporte (sensores que miden el pulso, bio-identificadores que reconocen a las personas y saben sus preferencias), Trabajo doméstico y aprendizaje (para ayudar a reducir la cantidad de trabajo a realizar). Un ejemplo del desarrollo del AmI en el hogar que proporciona un contexto con conciencia y que es proactivo en la ayuda a la realización de alguna de las actividades cotidianas es el presentado por *[Encarnacao, J.L. & Kirste, T. 2005]*, en el cual el espejo del cuarto de baño recuerda a la persona si se ha tomado su medicación.

Las tecnologías utilizadas en los dominios del AmI pueden aportar beneficios adicionales si se integran y combinan los datos biológicos y fisiológicos con otros datos acerca del usuario, obtenidos en la realización de las diferentes actividades de su vida cotidiana *[Haux, R. 2006]*. En este trabajo el autor muestra un especial énfasis en sustituir el término “atención de la salud” por el de “prevención de la salud”, en el que considera relevante el uso de las Tecnologías de la Información y la Comunicación (TIC).

Algunos patrones de comportamiento de los pacientes que afectan a la salud o que indican señales de deterioro, tanto físico como cognitivo, pueden no ser detectados fácilmente en un entorno médico (centro de salud, visita paciente), siendo solo detectables a través de su monitorización en la vivienda del paciente.

La Organización Mundial de la Salud, en su resolución eHealth del 2005 (World Health Assembly), insta a cada estado miembro a: esforzarse en extender a todas las comunidades de usuarios, incluidos los grupos vulnerables, los servicios de salud en línea eHealth (cibersalud) de acuerdo a sus necesidades, así como a desarrollar las infraestructuras de las TIC para la salud, de modo que promuevan el acceso equitativo, asequible y universal de sus beneficios, contribuyendo todas las partes implicadas, con el fin de reducir costos y hacer que el eHealth tenga éxito.

El proyecto Genio *[Garate, A. et al. 2005]* permite la realización de diferentes actividades en el hogar como: leer el correo electrónico, poner en marcha la lavadora, chequear los alimentos en buen estado en la nevera, elaborar la lista de la compra, preparar una receta, buscar una canción determinada. El Sistema está formado por pequeños electrodomésticos (dotados de tarjetas RFID), sensores, seguridad y aparatos de calefacción que forman una red gestionada por un controlador central llamado Maior-Domo (representado por un avatar), que está equipado con sistemas de reconocimiento del habla, texto, aplicaciones e información digital, para responder y dialogar con el usuario a través del micrófono inalámbrico que éste lleva consigo.

Un hogar inteligente que actúa como un sistema de agentes racionales que cooperan en la adquisición y utilización de la información sobre los habitantes para proporcionales confort (control de temperatura, ventilación, luces), y eficiencia (en términos del buen uso y rendimiento de servicios como el gas o la electricidad), es el presentado por *[Cook, D.J. et al. 2006]* en el proyecto MavHome (Managing An Intelligent Versatile Home). El sistema está formado por diversos sensores y actuadores distribuidos en el hogar que minimizan la interacción manual de los habitantes con los dispositivos de control. El sistema es capaz de identificar las tendencias del estilo de vida de los habitantes y predecir sus actividades futuras, proporcionándoles recordatorios y detectando posibles anomalías cuando los eventos recibidos a través de los sensores no están de acuerdo con las predicciones realizadas por el sistema.

Existen diferentes aplicaciones eHealth que ya han mejorado la calidad de vida de las personas. Por ejemplo, los médicos pueden ver radiografías a distancia, y ayudar o tratar a los pacientes por medio de robots a distancia *[Riva, G. 2003]*. También existe en la actualidad una amplia gama de dispositivos portátiles como sensores y micro sensores embebidos en la ropa, o insertados en cinturones o pulseras, que miden diferentes parámetros respiratorios, bioquímicos (nivel de glucosa), fisiológicos (ECG). En *[Gouaux, F. et al. 2002]* se expone el desarrollo de un monitor ECG personal (PEM) como parte del proyecto europeo "EPI-MEDICS" *[http://epi-medics.insa-lyon.fr/statico/epimedica.htm]* cuyo objetivo es detectar, lo antes posible, alteraciones cardiacas con el fin de reducir el tiempo de espera del tratamiento a utilizar.

En *[Muñoz, M.A. et al. 2003], [Favela, J. et al.2004]* y *[Rodríguez, M. et al. 2004, 2005]*, se presentan los estudios realizados en un hospital con la colaboración de los trabajadores del mismo que se desarrollan en tres escenarios: en dos de ellos los doctores se comunican y transmiten información médica a través de sus PDA, y en el tercero un paciente solicita la recomendación de un cardiólogo del hospital. La arquitectura para el cuidado de la salud descrita está basada en agentes que actúan en nombre de los usuarios y representan los diferentes servicios que proporciona la aplicación llamada SALSA, que muestra en la pantalla de una PDA el Sistema de Información del Hospital, utilizando una red local inalámbrica (WLAN) para la comunicación.

Un estudio cualitativo sobre el diseño de las tecnologías de la información para ayudar a los pacientes diabéticos en sus actividades cotidianas, es el presentado en *[Kanstrup, A.M. et al. 2008]*. En este trabajo se plantean aspectos como la cooperación entre los pacientes a través de la comunicación entre los dispositivos médicos, que les permite compartir información sobre sus pensamientos, problemas, inquietudes y experiencias. En el diseño de este proyecto MaXi-project, una cuestión importante que hay que tener en cuenta es mantener la privacidad y seguridad de los datos que se transfieren entre los pacientes.

UbiMeds *[Silva, J.M. et al. 2009]* es una aplicación móvil que permite a los pacientes acceder a información sobre la prescripción de medicinas a través de horarios, recordatorios y toma de medicación. En esta aplicación resulta importante considerar la privacidad, ya que la información sobre la salud recogida puede ser usada por terceras partes como Google Health o Microsoft Vault, que son los que ofrecen los servicios en la aplicación, almacenando los registros de salud grabados.

Un sistema personalizado que guía al paciente y a sus cuidadores para monitorizar su estado de salud, mediante una red de sensores, es el presentado por *[Heinzelman, W. et al. 2004].* La monitorización de la salud resulta particularmente beneficiosa tanto para los enfermos crónicos como para las personas mayores *[Jung, D. et al. 2005]*. Diferentes sensores capturan de manera automática información relacionada con la salud, como el ritmo cardíaco, la presión sanguínea, la localización de una persona en una determinada estancia, la toma de la medicación, etc., por lo que resulta necesario proteger estos datos frente a ataques externos, y hacer seguro el almacenamiento de los mismos, de tal forma que no se invada la privacidad de los usuarios.

GerAmI (Geriatric Ambient Intelligence) es un sistema basado en el desarrollo de un Sistema Multi-Agentes que facilita el cuidado de los pacientes de Alzheimer en una residencia *[Corchado, J.M. et al. 2008].* El sistema consta de lectores de identificación colocados en las puertas del centro, ascensores, y de pulseras de identificación provistas de chips RFID que llevan los pacientes y enfermeras. Además las enfermeras disponen de dispositivos móviles (PDA), que controlan también determinadas situaciones de alarmas y cierres controlados, así como diferentes puntos de acceso inalámbricos. El agente administrador del sistema y los agentes que representan a los pacientes se ejecutan en un ordenador central, y los agentes que representan a las enfermeras se ejecutan y gestionan a través de los dispositivos móviles. De esta forma la localización de los pacientes se encuentra registrada en la base de datos del sistema central, permitiendo a las enfermeras conocer en todo momento el lugar donde se encuentran los pacientes, y si se produce alguna emergencia.

Building Bridges es un proyecto que ofrece la conexión social entre las personas mayores y sus familiares y amigos, con el propósito de reducir el riesgo de soledad y de aislamiento social que puede sufrir este colectivo *[Doyle, J. et al. 2010]*. La comunicación entre las personas mayores y sus cuidadores, familiares y amigos se establece mediante una pantalla táctil a través de la cual se establecen llamadas y servicios de mensajes escritos, y una "sala de té" que representa un fórum de chat. El principal objetivo de esta aplicación se basa en el estudio de la usabilidad del dispositivo de comunicación propuesto.

En *[Niemela, M. et al. 2007]* se presenta un trabajo sobre diferentes aplicaciones relativas a la vigilancia de la salud y la seguridad en el hogar de las personas mayores mediante la utilización de los teléfonos móviles que realizan la lectura de diferentes sensores y etiquetas colocados en diferentes objetos. Los escenarios en los que se desarrolla el estudio son: la toma de medicinas, el sueño, y la seguridad en el hogar. En el primer escenario el usuario utiliza un pastillero inteligente (suministrado por el doctor), conectado a un teléfono móvil vía Bluetooth, en el que se muestra el tiempo transcurrido entre cada apertura y cierre del pastillero, controlando así la toma de las medicinas. Los datos son enviados a una base de datos en Internet, comunicada con el centro de atención a la salud, la cual notifica al doctor si el paciente no ha abierto el pastillero en varios días. En el segundo escenario, se controlan los casos de apnea del sueño, mediante la monitorización del sueño. El dispositivo utilizado es un sensor colocado en la frente del usuario que detecta las ondas cerebrales y los movimientos de la cabeza del paciente mientras duerme (electroencefalograma, EEG). Estos datos son enviados a un teléfono móvil que se encarga de transferirlos al centro de atención, donde se analizan y detectan posibles anomalías. En el tercer escenario, el hogar se encuentra dotado de diferentes sensores que monitorizan los movimientos de los habitantes en la casa, con el fin de detectar posibles comportamientos anómalos que son enviados mediante el teléfono móvil a un centro de seguridad.

En este estudio participaron personas mayores de Finlandia y de España, las cuales manifestaron su preocupación por los temas relacionados con la privacidad y seguridad de los sistemas desarrollados. Mientras el grupo finlandés se interesaba por la privacidad y seguridad en el modo en el que los sistemas recogían y almacenaban los

datos de los pacientes, el grupo español mostraba su preocupación por la confianza en los centros de atención de la salud y los de seguridad, para que accedieran a las viviendas en el caso de producirse alguna situación de alarma.

Una aplicación para promover el ejercicio físico entre las personas mayores se describe en el trabajo presentado por *[Carmichael, A. et al. 2010]*, mediante la utilización de una televisión digital conectada a un mini-PC, cámaras HD, web-camera, conexión inalámbrica por Bluetooth, y la videoconsola Nintendo Wii Fit. En este trabajo se presta especial atención a la usabilidad y aceptación de los usuarios como feedback de este colectivo, para mejorar el desarrollo de la aplicación.

La plataforma inalámbrica BeClose gestiona la salud y el bienestar de las personas mayores en sus hogares, facilitando la seguridad de la vida independiente de este colectivo *[Hanson, Mark A. et al. 2011]*. Mediante el uso de una red de sensores inalámbrica (detectores de movimiento Infrarrojos, detectores en puertas/armarios/camas/sillones/alfombras, y pulsadores de emergencia), se establece la comunicación con la estación base de monitorización de datos remotos, a través del teléfono móvil. Este centro de datos procesa la información recibida realizando de manera automática llamadas telefónicas, envío de mensajes de texto (SMS), notificaciones por e-mail, respuestas de emergencia, o mostrar información en un sitio web seguro desde el que se configura la notificación o respuesta personalizada.

Movital es un sistema móvil para la monitorización personal de signos vitales, que facilita la gestión en la terapia de la diabetes en pacientes diabéticos y/o personas mayores en su hogar *[A.J. Jara, et al. 2011]*. Mediante la utilización de tarjetas personales RFID, NFC que identifican a los pacientes, cargando el perfil sobre su estado de salud, la conectividad de las redes de sensores inalámbricas con dispositivos clínicos también inalámbricos (glucómetro), las aplicaciones de gestión de las tarjetas por el personal sanitario (dotadas de un identificador del sistema de gestión que ofrece mayor seguridad y privacidad), el sistema de información de los índices de glucemia y el portal web de los pacientes (que les permite consultar una lista de alimentos que

pueden ingerir según los niveles de azúcar medidos), se facilita el control de estos pacientes.

La utilización de los teléfonos móviles dotados de tecnología NFC se presenta en *[J. Sidén, et al. 2011]*. Estos teléfonos realizan la lectura de etiquetas pasivas NFC integradas en sensores alojados en diferentes objetos y dispositivos (termómetro, vendajes, pañales), obteniendo así información sobre diferentes parámetros del paciente, que es transferida a un servidor web sin necesidad de tener que iniciar ninguna aplicación especial, ni accionar ningún botón en el teléfono móvil.

El Sistema de Información del Ambiente (AIS) presentado por *[Marcela D. Rodríguez, et al. 2011]* ofrece ayuda a las personas mayores en la toma de sus medicinas. El sistema consta de tres componentes: CARE-Me (Context Aware Representation of Elderly Medication), que se encuentra embebido en un marco de fotos con un nido virtual de periquitos que debe cuidar (cada periquito se encuentra asociado con cada semana del mes). Remind-Me (Remind elders to Medicate), teléfono móvil que emite un recordatorio sonoro de la medicina que debe tomar junto a una imagen del alimento que provoca un aumento en ese problema de salud. Y por último, un conjunto de interfaces geométricos que se iluminan, GUIDE-Me (Geometric User Interfaces to Display aids for the Elderly when Medicating), y que se encuentran vinculados a cada medicina que el usuario debe tomarse. De esta forma, cuando la persona va a acostarse, el sonido del Remind-Me le recuerda que debe tomarse sus medicinas, se acerca a sus medicinas y ve el GUIDE-Me iluminado en las medicinas que debe tomarse, y mirando el CARE-Me comprueba la correcta evolución del nido.

3.4.2. Educación

Las capacidades de aprendizaje de los usuarios pueden verse incrementadas con el uso de los dispositivos móviles como los Smartphone, ya que ofrecen libertad al usuario para ampliar sus conocimientos sin necesidad de tener que encontrarse en una localización determinada. Se conoce con el nombre de mobile learning (m-learning) a la combinación entre el e-learning y la computación móvil *[Holzinger, A. et al, 2005]*.

El sistema desarrollado en m-learning permite interaccionar con material de aprendizaje en diferentes modos, a la vez que explora el entorno físico, ya sea exterior (parque arqueológico, bosques) o interior (laboratorio, hogar) *[Rogers, Y. et al. 2005]*.

El proyecto Explore! *[Costabile, María F. et al. 2008]* es un sistema de aprendizaje móvil que implementa un juego en el que participan estudiantes de secundaria durante una visita a un parque arqueológico. Este sistema de aprendizaje está basado en Teaching History *[Ciancio, E. et. al. 2000]*. A través del sistema móvil-learning se intercambian los datos entre el teléfono móvil y la tarjeta de memoria interna, facilitando a los estudiantes el aprendizaje de la historia mientras realizan su visita al parque arqueológico.

El estudio presentado en *[Aroyo, L & Kommers, P. 2001]*, propone un modelo de aprendizaje interactivo basado en Agentes inteligentes. Otro modelo de Agentes inteligentes animados es el que se detalla en *[Johnson W.L., Rickel J.W. & Lester J.C. 2000]* en el que, gracias a las capacidades de interacción de los agentes y a su aprendizaje del entorno, se promueve la motivación y atención de los estudiantes.

Una aplicación desarrollada en una PDA llamada Mistery in the Museum *[Klopfer, E. et al. 2005]* estimula la colaboración entre grupos de estudiantes al interaccionar a través de un juego de misterio que se desarrolla con la visita a un museo. Mediante esta aplicación se estimula además la imaginación de los estudiantes.

En *[S. Sun, M.S. Joy, 2005]*, se presenta un sistema Multi-Agentes para facilitar el proceso de aprendizaje y enseñanza, mediante objetos que se adaptan a los requerimientos de los estudiantes, ofreciendo un sistema tutorial individualizado y personalizado para el aprendizaje.

Kurio es un sistema de guiado que mejora la interacción social y el aprendizaje de las familias en sus visitas a los museos *[R. Wakkary, et al. 2009]*. El sistema es una guía interactiva para familias y pequeños grupos, embebida en una interface de usuario tangible que se encuentra distribuida en varios dispositivos computacionales (Tablet, PDA) con arquitectura cliente/servidor, centrada en la comunicación entre estos dispositivos a través de una red WiFi. Mediante esta guía, los participantes llevan a cabo una serie de retos recopilando información del museo que les permite la realización de un plano del mismo. En este sistema se encuentran sensores de Infrarrojos colocados en diferentes objetos del museo, lectores y etiquetas RFID que se encuentran en pequeños iconos que ilustran la diferente información que ofrece el museo.

Un estudio sobre la investigación de la computación ubicua en el dominio de aplicación del mobile-learning se presenta en *[C.X. Navarro, et al. 2015]*. La evaluación de las aplicaciones m-learning, teniendo en cuenta consideraciones pedagógicas y de usabilidad, permite mejorar la calidad en la utilización de estas aplicaciones, y así mejorar y estimular el aprendizaje del usuario en este entorno.

3.4.3. Comercio y Negocios/ Servicios Públicos y Transporte/ Sistemas de Recomendación

El comportamiento reactivo que presentan los entornos interactivos del AmI, capaces de detectar la existencia de eventos y reaccionar a ellos mediante la combinación entre el mundo físico y los agentes software, es el utilizado en la aplicación presentada por *[Da Silva, F.S. and Vasconcelos, W.W. 2007]*, en la que consideran el comercio como un entorno interactivo. La aplicación que describen es una librería equipada con sensores distribuidos entre los libros y en diferentes lugares de la tienda, que detectan e identifican a los clientes a través de sus dispositivos portátiles (Smartphone con Bluetooth, PDA, Tarjetas de fidelidad de la tienda).
La tienda descrita tiene información acerca del perfil de sus clientes, de los últimos libros que han comprado, de sus gustos, asociando de esta forma la identidad del cliente con su perfil. Con toda esta información se mejora la estancia de los clientes en

la tienda (reproductores de música y pantallas LCD dispuestas por la tienda), y se estimula o fomenta la realización de compras por los mismos, maximizando así las ventas. Una continuación de este sistema es el presentado por *[Masthoff, J. et al. 2007]*, que se encuentra enfocado en su mayor parte, en múltiples clientes que interaccionan con una amplia gama de dispositivos de detección e identificación.

La interacción entre los dispositivos móviles equipados de tecnología NFC (Near Field Communication) y los espacios físicos, es la que aparece descrita en *[A. Geven, et al. 2007]*. En este trabajo se muestran las posibilidades que ofrece la tecnología NFC presente en los dispositivos móviles, dentro de diferentes entornos relacionados con el comercio, tiendas, ocio y entretenimiento.

En *[Kopacsi, S. et al. 2007]* se analizan las posibilidades que ofrece la Inteligencia Ambiental en los procesos de fabricación. Gracias a la utilización de diferentes sensores en los procesos de producción de las empresas, es posible obtener y almacenar información de forma continua, sobre las diferentes etapas que conforman el proceso de producción y sobre los productos finales que se elaboran en una empresa. El almacenaje de esta información permite su posterior análisis y gestión, que ayuda en la toma de decisiones para prevenir un posible riesgo de fallo tanto en la cadena de producción como en la elaboración final de algún producto similar a los almacenados.

Un resumen de proyectos industriales desarrollados en AmI es el presentado en *[Werner Weber, 2003]*. Estas aplicaciones incluyen la integración de diferentes dispositivos electrónicos en el proceso de fabricación de ropa, alfombras o ropa de cama. Como ejemplos tenemos una chaqueta en la que se encuentra incrustado un reproductor MP3 provisto de teclado, auriculares, micrófono y batería; un dispositivo que convierte el calor corporal en energía que, aunque se produce en poca cantidad, es suficiente para poner en marcha un reloj de pulsera o un sensor del ritmo cardíaco; otro ejemplo es una tela que contiene una red distribuida de unidades electrónicas tejidas en ella que podría usarse en alfombras y revestimientos de suelos, para la detección y vigilancia, o como guías en algunos edificios, o para monitorizar las

constantes vitales de los pacientes de un hospital.

El sistema Easishop, *[Keegan, S. et al. 2008]* tiene como objetivo facilitar el intercambio de la información dependiente del contexto y de negociación entre los comercios y los clientes. La arquitectura se basa en una estructura Multiagente BDI (Believes, Desires and Intentions). Cada cliente y cada comercio tienen su propio agente, la comunicación entre los agentes es vía Bluetooth. Los dispositivos de los clientes son teléfonos móviles y PDA.

Una aplicación para gestionar de manera automática el equipaje de un aeropuerto es la que se presenta en *[P. DeVries, 2008]*. El objetivo principal es la gestión del transporte del equipaje a través de los transportadores, carros y aviones a su destino correcto. El equipaje se marca al hacer el Check-In con tarjetas RFID. En esta aplicación, resulta importante tener en consideración cuestiones relacionadas con la visibilidad, seguridad y protección de la información de estas tarjetas.

En Driving, *[Bosse, T. et al. 2008]*, se describe un sistema de agentes para vigilar (monitorizar) el comportamiento de los conductores. El objetivo de la aplicación es detectar si, con el paso del tiempo se deteriora la conducción mediante la toma de lecturas periódicas del manejo del volante por parte del conductor y de los sitios hacia los que dirige su mirada durante la conducción, de tal forma que, si detecta que la conducción se deteriora, hace que el automóvil vaya reduciendo su velocidad llegando incluso a detenerse y cortar el contacto si fuera necesario.

Una aplicación para el control de la carga en una red de transporte de trenes es la que aparece descrita en *[J. Reason & R. Crepaldi, 2009]*. En esta aplicación, los vagones de carga de los trenes se encuentran dotados de una variedad de sensores que controlan las condiciones de la carga. Todos los eventos detectados se comunican a través de una red de sensores inalámbrica con la estación central. Debido a la naturaleza crítica sobre la seguridad y a los requerimientos de privacidad de algunos de estos eventos, resulta importante ofrecer una notificación segura de los mismos.

En *[Tomás Sánchez López et al. 2011]*, se presenta un prototipo de logística de transporte para el seguimiento en tiempo real de mercancías perecederas en una cadena de suministro. Gracias a la integración de Smart Objects (provistos de tarjetas RFID), sensores, objetos embebidos y servicios de Internet, se gestiona de una manera distribuida la red de transporte de las mercancías, a través de redes de sensores inalámbricas y servicios web que permiten, además de reducir gastos y residuos, agilizar situaciones de manera autónoma, lo cual ofrece un valor añadido a la eficacia del servicio.

Los grupos e instituciones involucrados en la toma de decisiones, en los que se combinan las personas y los sistemas computacionales (llamados agentes), representan en la actualidad una de las áreas de la Inteligencia Ambiental más investigada en el desarrollo de los Entornos Inteligentes. Un ejemplo de aplicación de este tipo de sistemas de recomendación para la toma de decisiones en grupos es el relativo al cuidado de la salud presentado por *[Karacapilidis, N. and Papadias, D. 2001]*, en el que el tratamiento de los pacientes involucra a diferentes especialistas de varios departamentos.

Los autores *[Prakken, H. and Gordon, T.F. 1999]* proponen un sistema de mediación automatizado para la toma de decisiones, aplicado al proceso de la planificación urbana en el proyecto europeo llamado GeoMed. El objetivo del sistema es la monitorización de las reuniones que tienen lugar entre los miembros del proyecto, recordándoles cuáles van a ser las acciones previstas a realizar, y notificándoles cuándo se incumplen las reglas que han sido establecidas por el grupo.

En los trabajos presentados por *[Gonzalez, G. et al. 2004a, 2004b, 2005, 2006],* se analizan los sistemas de recomendación centrándose en la forma de proporcionar información personalizada, sin necesidad de aumentar la retroalimentación directa, ni las entradas del usuario. Dichos sistemas de recomendación se basan en la captura de los datos del usuario de una forma genérica, a través de un modelo llamado Smart User Model (SUM), que permite transferir estos datos, desde un dominio en el que se ha elaborado el perfil del usuario, a otro dominio en el cual dicho perfil no se

encuentra definido. Este modelo de usuario se divide en tres categorías según la naturaleza de los datos adquiridos: objetiva (edad, sexo, país), subjetiva (gustos), y emocional (no contemplada en el estudio presentado). Los atributos objetivos pueden ser proporcionados por el usuario y obtenidos a través de una base de datos, y los subjetivos son adquiridos a través de las interacciones que realiza el usuario con el entorno.

3.4.4. Ocio y Entretenimiento

En la última década, se han producido importantes avances en la industria del turismo, en lo que se refiere a la provisión de ofrecer servicios de información personalizados a los usuarios *[Rumetshofer, H. et al. 2003]*.

A la hora de desarrollar las aplicaciones del AmI orientadas al turismo, hay que tener en cuenta las características de los dos tipos de entornos en los que puede implementarse, ya sean de interior o de exterior *[Manes, G. 2003]*, *[Staab, S. et. al. 2002]*. En el interior (museos, estaciones de servicios de transporte), los usuarios obtienen diferentes tipos de servicios de información sobre horarios, tiempos de espera, adquisición de billetes, etc., a través de paneles informativos colocados en diferentes sitios, mediante la utilización de su dispositivo móvil provisto de tecnología NFC *[Oyster mobile wallet, Londor underground, 2008]*, *[Monaco City Museum, 2009]*. En el exterior, para la adquisición de este tipo de servicios, suelen utilizarse tecnologías GPS o planos de realidad aumentada provistos de etiquetas RFID *[Liikka, J. et al. 2008]*.

La utilización de las TICs (Tecnologías de la Información y las Comunicaciones) en el desarrollo de un sistema turístico, a través de la localización mediante dispositivos móviles, es el presentado en *[Bojen Nielsen, L.MA. 2004].* El proyecto se centra tanto en el contenido, como en la información, productos y servicios que pueden ofrecerse a los turistas a través del desarrollo de diferentes tipos de contenidos en una plataforma móvil (Smartphone, Tablet). Las soluciones ofrecidas a través de esta plataforma son interactivas, y están orientadas en las necesidades de los clientes y de los operadores turísticos, lo cual requiere una retroalimentación cualitativa que permita mejorar y desarrollar la información personalizada de los servicios turísticos móviles ofrecidos.

Resulta importante destacar la consideración de cuestiones éticas que pueden derivarse de la adquisición de los datos de los clientes a través de los dispositivos móviles.

En *[Penserini, L. et al. 2005],* se presenta la arquitectura de un sistema Multiagente implementado en un entorno sensible/activo, que forma parte del proyecto Peach (Personal Experience with Active Cultural Heritage) llevado a cabo por Italia, Alemania, USA y Canadá. El escenario elegido es el de un visitante de un museo, que solicita vía PDA una presentación de alguna de las exposiciones que hay en el museo. Los facilitadores de los servicios ofrecidos, modelados como agentes, son capaces de realizar dicha presentación mediante imágenes, audio, video o la combinación de audio y video. Cuando el visitante se encuentra cerca de alguno de estos facilitadores, que pueden ser por ejemplo pantallas o altavoces, puede también obtener en la pantalla de su PDA la presentación solicitada.

Dos aplicaciones relacionadas con lugares de patrimonio cultural se describen en *[Constantini, S. et al. 2008]*. En este trabajo se combina el uso de la tecnología Multiagente con sensores y satélites de seguimiento, y una PDA para el desarrollo e implementación de dos aplicaciones relacionadas con el patrimonio. Una de las aplicaciones se basa en la provisión de información a los visitantes de una antigua villa romana (Villa Adrianna), en la que el sistema Multiagente desarrollado llamado DALICA, utiliza una representación del sitio con los lugares de mayor interés, ofreciendo al visitante información sobre lo que más le puede interesar, basándose en el tiempo que cada visitante permanece observando cada lugar, y en la confirmación del usuario en su interés por cada sitio.

La comunicación con el usuario se establece a través de una PDA, y el seguimiento de la localización se realiza vía satélite. La otra aplicación presentada se centra en el seguimiento de objetos pertenecientes al patrimonio cultural durante su transporte, con el objetivo de evitar su robo y de mantener las condiciones óptimas de temperatura y humedad para su conservación. Para ello, cada paquete se encuentra equipado con un dispositivo móvil que de manera periódica chequea la temperatura y la humedad del mismo, así como la posición en la que se encuentra el paquete.

Este dispositivo móvil también efectúa un control sobre la ruta que sigue el paquete, facilitada vía satélite, verificándose así que se sigue la ruta acordada y no se produce ninguna alteración en la misma. Cualquier anomalía que se origine en la adquisición de estos parámetros de control, se traduciría en el envío de mensajes de advertencia o peligro.

Una aplicación para el guiado de turistas por la ciudad de Trondheim (Noruega) se presenta en *[Petersen, S. and Kofod-Petersen, A. 2006]*. El objetivo principal del trabajo presentado es que el turista pueda ver y disfrutar de la ciudad en un solo día, lo cual es posible gracias a la selección que puede realizar a través de la aplicación desarrollada en una PDA, en la que puede seleccionar algunos puntos clave de su interés: Trondheim medieval, comida, tiendas, etc. Cuando el turista llega a Trondheim, dispone a través de una PDA de información sobre las experiencias que puede vivir en la ciudad (Trondheim Experience, TE). El turista puede planificar mediante TE su visita seleccionando diferentes actividades. La información ofrecida al turista proviene de empresas virtuales (Ves, Virtual enterprises) formadas por diferentes empresas de la ciudad y proveedores de servicios (guías para visita al museo, concierto en la catedral, comida en restaurante, compañía de taxi, centro comercial). Estas empresas virtuales pueden acceder al perfil del turista recogido por el Trondheim Experience y ofrecerle, así, el paquete de actividades compatible con su perfil. Cuando el turista escoge un paquete de actividades, el Trondheim Experience guía al turista en el desarrollo de las diferentes actividades propuestas, pudiendo también utilizar los seguidores de localización para proporcionarle información acerca de la arquitectura o historia de los edificios, tiendas, así como diferentes ofertas que puede aprovechar mientras dura su estancia en la ciudad.

En *[Borrejo-Jaraba, F. et al. 2010]* se presenta una aplicación turística para visitar la ciudad de Córdoba, España. La propuesta se basa en el uso de la telefonía móvil provista de tecnología NFC para interaccionar con escenarios inteligentes, que sirven de guía para visitar la ciudad. Estos escenarios están formados por carteles inteligentes (Smart Posters) provistos de etiquetas RFID con información escrita y visual acerca de lugares que el turista podría visitar.

El usuario interacciona con estos carteles a través de su teléfono móvil, de un modo fácil, intuitivo y con consciencia del contexto, que le ofrece información sobre dónde se encuentra, lo que está viendo, y lo que hay cerca de su localización, permitiéndole además diseñar su propia ruta para visitar la ciudad.

3.5. PRINCIPALES TECNOLOGÍAS DEL AmI

Las tecnologías utilizadas en el desarrollo de las aplicaciones del AmI se basan en diferentes dispositivos de computación y de comunicación que tienen la capacidad de adquirir, almacenar, gestionar y transmitir diferentes tipos de información sobre el usuario y el contexto en el que éste se encuentra. Estas capacidades les permiten comunicarse entre ellos y también comunicarse con el usuario. Todos los dispositivos que forman parte de un Entorno Inteligente propio de la Inteligencia Ambiental o Computación Ubicua, interaccionan entre sí y con el usuario a través de las comunicaciones ubicuas que permiten al usuario el acceso a los servicios computacionales ofrecidos desde cualquier lugar en el que se encuentre. Además, las comunicaciones ubicuas obtienen y proporcionan diferentes tipos de información a los usuarios, gracias a los dispositivos que se encuentran dispersos en el entorno, minimizando así la intervención explícita de los usuarios. La finalidad fundamental de estos dispositivos de computación es que puedan comunicarse entre sí y con el usuario, para ofrecer mayor número y calidad de servicios.

La tecnología presente en los dominios de aplicación del AmI se basa en la miniaturización y en el bajo coste de los dispositivos de hardware utilizados, lo cual proporciona complejas redes de computación y comunicación de la información, en un entorno que se caracteriza por ser heterogéneo, distribuido y dinámico.

Las principales tecnologías utilizadas en el desarrollo de las aplicaciones del AmI estudiadas, han sido agrupadas en las siguientes categorías: Sensores inteligentes, Redes de comunicación inalámbricas, Interfaces de usuario inteligentes, y Plataformas Inteligentes.

3.5.1. Sensores inteligentes

Las redes de sensores inteligentes destacan como uno de los dispositivos de computación ubicua más utilizados en los dominios de aplicación de la Inteligencia Ambiental (Capítulo 1, Introducción). Estas redes de sensores representan una de las tecnologías más prometedoras del futuro debido, sobre todo, al bajo coste en su desarrollo, los avances en nanotecnología, su portabilidad, y sobre todo a su gran capacidad de comunicación, por lo que su campo de aplicación cada vez está más extendido. Se estima que en el año 2020 habrá cerca de 50.000 millones de este tipo de dispositivos conectados según el informe presentado por la compañía Ericsson, lo cual representa aproximadamente 70 conexiones de dispositivos computacionales por persona *[El internet de las cosas. Monográfico de la revista BIT, nº 187, 2011].*

En la actualidad, las redes de sensores inalámbricas (Wireless Sensor Networks, WSNs) se encuentran ampliamente extendidas en diferentes sectores, gracias a su capacidad para automatizar la recogida de datos, la monitorización, vigilancia y control de los sistemas involucrados en la operativa de sectores como el financiero (Terminales de Punto de Venta, Cajeros automáticos, Tarjetas de pago), la seguridad (alarmas y sistemas de tele vigilancia), redes de distribución de energía (telecontrol), los sistemas de gestión y control de flotas de medios de transporte, etc.

Estos dispositivos computacionales son capaces de analizar y obtener información del usuario y del entorno que le rodea, en cualquier lugar y momento (gracias a su portabilidad), adaptándose en consecuencia y llegando a anticiparse a los requerimientos o necesidades del usuario. Algunos de los parámetros principales que caracterizan a los sensores son: flexibilidad, robustez, seguridad, capacidad de computación, capacidad de comunicación, facilidad para la sincronización, tamaño y coste, y el gasto energético.

La información que adquieren las redes de sensores inteligentes del usuario y del entorno en el que se encuentra, presenta distinta naturaleza pudiendo estar relacionada con datos fisiológicos del usuario (ritmo cardíaco, niveles de oxígeno, etc.), datos biométricos (huella dactilar, voz, forma de andar, etc.), datos sobre su posición y localización, así como la relacionada con el entorno que le rodea (luminosidad, sonoridad, etc.).

La tecnología de las redes de sensores corporales es la utilizada en los trabajos presentados en *[Min Chen, et al. 2011]*, *[A. Weder, et al. 2011]*, *[J. Espina, et al. 2008]*. Otros estudios sobre la utilización de las redes de sensores son los realizados por *[Veselin Ganev, et al. 2011], [J.S. Bermúdez et al. 2011]*, *[Jeffrey W. Lockhart, et al. 2011]*.

Según la naturaleza de los datos obtenidos en las aplicaciones del AmI estudiadas, hemos establecido la siguiente clasificación de los sensores: Sensores vitales, Sensores biométricos, Sensores de comportamiento, y Sensores ambientales.

- **Sensores vitales:** Estos sensores son capaces de detectar la actividad nerviosa y muscular de los usuarios, adquiriendo datos relacionados con parámetros fisiológicos de éstos. El gran avance desarrollado en este tipo de sensores ha permitido mejorar la calidad de vida de los usuarios, ya que es posible realizar el seguimiento de dichos parámetros desde el propio domicilio, mediante los servicios de tele-asistencia. Entre este tipo de dispositivos tenemos: monitores de electrocardiograma, glucómetros, medidores de presión arterial y frecuencia cardiaca, básculas digitales, pulsioxímetros e incluso monitores para el control de actividad, ejercicio físico o rehabilitación muscular, etc.

Figura 3.3. Sensores vitales. De izda. a dcha.: glucómetro, tensiómetro, pulsioxímetro

Figura 3.4. Glucómetro conectado a consola de videojuegos

- **Sensores biométricos:** Estos sensores son capaces de reconocer o identificar en tiempo real a las personas que se encuentran en un determinado entorno, mediante el análisis de sus características biométricas (modulación de la voz, iris, gestos habituales, huella dactilar y/o digital, etc.). El reconocimiento de personas a partir de sus rasgos biométricos se encuentra cada vez más extendido en nuestra sociedad, estando presente en aplicaciones de seguridad, privacidad e interacción human-computer; siendo la investigación de nuevos algoritmos y técnicas que permitan la implementación de sistemas multimodales atendiendo al nivel de fusión de los diferentes rasgos biométricos, uno de los campos con más potencial de desarrollo para la identificación de personas de una manera fiable y segura.

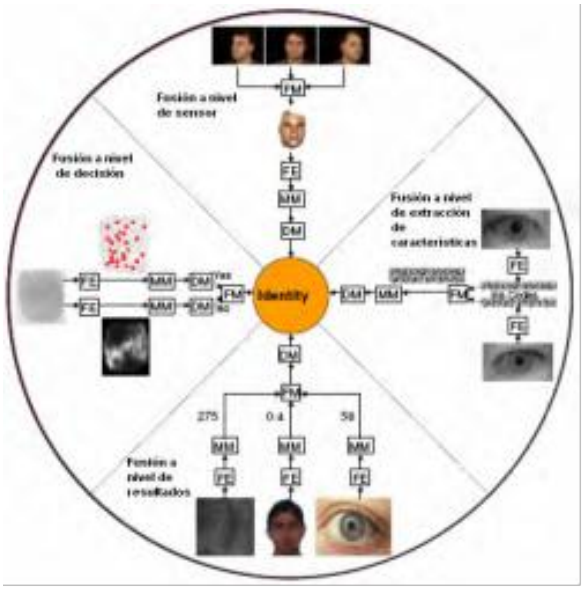

Figura 3.5. Representación de los niveles de fusión de los sistemas de biometría multimodal

A partir del nivel de fusión de la información, podemos disponer de diferentes tipos de información (rasgos, sensores, algoritmos) en diferentes niveles (a nivel de sensores, de parámetros o características, de resultados y de nivel de decisiones).

En el desarrollo de los sistemas biométricos multimodales resulta necesario analizar tanto el tipo de aplicación como el nivel de seguridad que ésta requiere, a la hora de decidir si se opta por un sistema biométrico tradicional (con un solo parámetro o característica), o por uno más complejo que fusione diferentes características (multimodal).

- **Sensores de comportamiento:** La información obtenida por este tipo de dispositivos se refiere al estado del usuario en un ámbito más general, como puede ser la posición en la que está, o su localización. Dentro de este tipo de sensores, nos encontramos con: Sensores y dispositivos de localización, Sensores de detección de caídas, y Dispositivos de aviso de socorro.

Figura 3.6. Sensores de comportamiento. De izda. a dcha.: sensor de localización (IR), sensor de detección de caídas y dispositivo de aviso de socorro.

Los sensores y dispositivos de localización son los encargados de detectar la posición y localización del usuario, que puede ser monitorizada por terceras personas de forma remota. Esta localización puede obtenerse desde sistemas que integran la tecnología GPS (Global Positioning Systems) para localización de exteriores, hasta de sensores de presencia (Detección por Infrarrojos) que permiten detectar si el usuario se encuentra en casa e incluso en qué lugar de la misma se encuentra en todo momento. Actualmente, una de las tendencias más utilizadas consiste en la incorporación de sistemas de visión artificial en entornos de domótica, gracias a la utilización de cámaras y al gran avance en velocidad computacional de los ordenadores actuales. De esta forma, es posible detectar la presencia del usuario en un determinado entorno e incluso obtener información adicional de manera automática (por ejemplo, si está solo o acompañado), además de poder visualizar las diferentes estancias del lugar en el que se encuentra de forma remota, en cualquier momento y en tiempo real.

Los sensores de detección de caídas, permiten detectar el riesgo de caídas así como las que ya han tenido lugar. Este tipo de sensores constan de un acelerómetro que se encuentra insertado en dispositivos que llevan los usuarios consigo en todo momento, de tal forma que cuando detectan un movimiento anómalo, activan una señal de alarma en el centro de tele-asistencia correspondiente.

La tendencia actual en este tipo de dispositivos es la de incorporar sistemas de visión artificial que detecten de manera automática las caídas y generen la alarma correspondiente, de tal forma que no sea necesario que el usuario lleve consigo ningún dispositivo.

Por último, tenemos los dispositivos de aviso de socorro. Este tipo de dispositivos son activados por el usuario de manera voluntaria cuando detecta que existe algún peligro o cuando necesita ayuda. Pueden ser fijos (conectados a la línea telefónica) o móviles (pulsador colgado del cuello o alojado en una pulsera). Cuando estos dispositivos son activados, se genera una señal de alarma que se transmite al centro de tele-asistencia correspondiente, para una rápida actuación.

En la siguiente figura se muestran algunos ejemplos de los últimos avances para la obtención de información relativa al comportamiento de los usuarios:

Figura 3.7. Obtención de información del comportamiento del usuario. De izda. a dcha.: detección de caídas visión artificial, dispositivo Kinect y teléfono móvil inteligente

- **Sensores ambientales:** Este tipo de sensores permiten detectar los valores ambientales del entorno en el que se encuentra el usuario, comprobando así, que se encuentran dentro de los parámetros de habitabilidad correctos y que no suponen un riesgo para el usuario. Algunos de los parámetros que miden los sensores ambientales son: la temperatura, la luminosidad, la humedad, el ruido, las inundaciones, la presencia de humo, de fuego, de gas, etc.

Los valores ambientales recogidos por este tipo de sensores son analizados, lo cual les permite generar alarmas automáticas en el caso de que se encuentren fuera de los rangos de confort y/o seguridad establecidos, así como activar los diferentes dispositivos habilitados para corregir o gestionar dichas anomalías.

Los sistemas de visión artificial vuelven a ser una tendencia actual en la detección de algunos de estos parámetros ambientales, como puede ser el caso de la detección de incendios. La ventaja de utilizar estos sistemas frente a los detectores de humo tradicionales, reside en que son capaces de detectar el humo o el fuego de forma visual, a diferencia de los sensores tradicionales que no detectan el incendio hasta que el humo alcanza al sensor, por lo que la activación de la alarma se genera de manera más rápida, llegando a ser capaces de activar de manera automática extintores para sofocar el fuego.

Figura 3.8. Sensores ambientales. De izda. a dcha.: sensor de gas, sensor de luminosidad, sensor de humo y sensor de inundación.

Las redes de sensores inteligentes instaladas en entornos como el hogar permite la captación de información del usuario relacionada con su actividad y sus patrones de comportamiento. Estos dispositivos de computación y comunicación pueden encontrarse embebidos (wereable computers) en una gran variedad de objetos que utilizamos de forma cotidiana llegando a estar, en muchos casos, ocultos para el usuario, lo cual conlleva un importante impacto social que requiere ser considerado.

Las redes de sensores inalámbricas, WSNs (Wireless Sensor Networks) constituyen uno de los campos de investigación más fructíferos de los últimos 15 años gracias a su amplio rango de aplicaciones, versatilidad y movilidad. Estas redes de sensores pueden ser clasificadas atendiendo a su naturaleza en tres tipos: homogéneas, heterogéneas y lineales *[I. Akyildiz, et al. 2002]*. En este tipo de redes cabe destacar, como una de las aplicaciones que ha suscitado mayor interés en la última década, la integración de las redes inalámbricas en Internet conocida como Sensor Web *[M. Gaynor, et al. 2004]*. En la siguiente figura se muestra la arquitectura típica de una Sensor Web, con sus componentes principales: sensor, puerta de enlace, estación base, servidor y clientes.

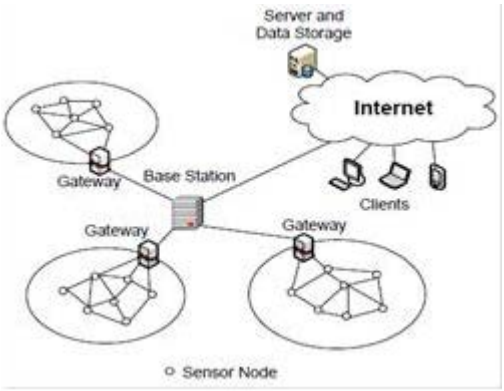

Figura 3.9. Arquitectura de una red típica de Sensor Web

Gracias a la utilización de este tipo de aplicaciones Sensor Web, es posible ofrecer mejoras en los servicios relacionados con el cuidado de la salud, la gestión de crisis (desastres), las redes sociales, etc., ya que permiten procesar la información en tiempo real, facilitando la gestión de los datos, y proporcionando algoritmos fiables a los sensores para localizar al usuario.

En *[E. Gavin, et. al. 2009]* se presenta una aplicación para el cuidado de la salud basado en Sensor Web: varios sensores colocados alrededor del paciente y de su cuerpo detectan diferentes atributos como la presión sanguínea, la temperatura, etc. y las envían a la web para ser analizadas por un especialista o médico. Cuando el paciente sale de su casa, los datos son almacenados en su dispositivo móvil, proporcionando una supervisión continua del estado del mismo.

El sistema Sensor Web propuesto en *[S. Patel et al. 2010]* se utilizó para la supervisión de pacientes con Parkinson: los sensores colocados en el paciente captan la velocidad de los movimientos de éste y los envían a la estación base del domicilio del paciente que a su vez remite esta información a la aplicación web, para ser supervisada por los especialistas en tiempo real.

El sistema de vigilancia de incendios forestales FFSS (Forest-Fire Surveillance System) presentado en *[B. Son, et al. 2006]* utiliza una red de sensores inalámbrica para recoger datos sobre temperatura y humedad, así como sobre detección de humo en el bosque. Esta información se recibe en la aplicación basada en la web que los analiza para extraer conclusiones sobre la situación. La red de sensores inalámbrica se encuentra conectada a Internet para el almacenamiento de los datos y para poder realizar futuros análisis y usos. En *[N. Markovic, et al. 2009]* se presenta un sistema de alerta para la vigilancia del agua de los ríos que detecta la contaminación presente, RWMAS (River Water Monitoring Alert System): los datos obtenidos por los sensores proporcionan información sobre el porcentaje de contaminación que hay en el agua, de qué tipo es y dónde se localiza. Todos estos datos ayudan en la toma de decisiones sobre el grado de contaminación del agua, su origen y causas.

CenceMe System *[E. Miluzzo, et al. 2008]* es un sistema que detecta el estado del usuario y lo publica en la cuenta de éste de cualquier red social. Los datos obtenidos son básicamente datos sobre la actividad desarrollada por el usuario y su localización. El sistema proporciona una configuración de la privacidad GUI, en la que el usuario puede seleccionar el tipo de datos que quiere compartir (audio, imágenes, localización), pero no puede seleccionar con quién quiere compartirlos. El sistema Whozthat *[A. Beach, et al. 2008]* combina la red web de sensores con las redes sociales para obtener información de cualquier persona del entorno del usuario que pueda ser de su interés. Utiliza como sensores los teléfonos móviles y como web las redes sociales. El sistema no proporciona un método seguro para el envío y recepción de los datos.

Algunos de los retos más destacados a los que debe atenderse en la aplicación de las redes de sensores inteligentes son la interoperabilidad de los datos, y la heterogeneidad de los dispositivos de computación y comunicación. Por ello, resulta necesario una estandarización e integración de este tipo de dispositivos que, además de normalizar los aspectos técnicos, regule con normas específicas los aspectos relacionados con la seguridad y protección de la información. Los sistemas desarrollados mediante la utilización de las redes de sensores deben proporcionar confianza, seguridad y privacidad tanto en la adquisición de los datos como en la transmisión de los mismos.

3.5.2. Redes de comunicación inalámbricas

Las redes de comunicación inalámbrica que generalmente se utilizan para dar soporte a la comunicación ubicua de los entornos desarrollados en Inteligencia Ambiental son: Redes de Área Corporal (WBAN, Wireless Body Area Networks), Redes de Área Personal (WPAN, Wireless Personal Area Networks), Redes de Área Local (WLAN, Wireless Local Area Networks), Redes de Área Ampliada (WWAN, Wireless Wide Area Networks), y las Redes del Mundo Virtual (Capítulo 1, Introducción).

Entre las Redes de Área Corporal, WBAN utilizadas en las aplicaciones del AmI, nos encontramos con diferentes tipos de dispositivos portables como sensores, chips, interfaces integrados en la ropa o colocados en alguna parte del cuerpo del usuario. El alcance de este tipo de redes es de aproximadamente 1 metro.

Las Redes de Área Personal, WPAN conectan dispositivos periféricos de entada/salida en un área de corto alcance de unos 10 metros. Entre los dispositivos que utilizan este tipo de comunicación, nos encontramos con los teléfonos móviles, los portátiles, etc. En las aplicaciones del AmI destacan dentro de estas redes, la comunicación por Zigbee y la comunicación por Bluetooth.

Las Redes de Área Local, WLAN ofrecen acceso tanto a redes fijas y móviles, conectándose a Internet a través de los puertos de comunicación habilitados. La distancia que alcanzan este tipo de redes suele ser de 2 a 200 metros. Dentro de este tipo de redes destaca el protocolo WiFi y las tarjetas o chips activas RFID, como los más utilizados en las aplicaciones del AmI estudiadas.

Gracias al enrutamiento global y a los protocolos de transporte, las Redes de Área Ampliada (WWAN) facilitan la movilidad del usuario, pudiendo alcanzar cualquier distancia en el mundo. Este tipo de redes inalámbricas permite compartir dispositivos, a través de un acceso rápido y eficaz, proporcionando una transmisión a larga distancia de datos, voz, imágenes y videos, en grandes áreas geográficas que pueden llegar a extenderse hacia un país, continente o el mundo entero. En este tipo de redes, la transmisión de la información se realiza generalmente a través de la fibra óptica y de los satélites. Entre estas redes destacan la tecnología UMTS (Universal Mobile Telecommunications Systems), utilizada por los teléfonos móviles de tercera y cuarta generación (3G y 4G), que ofrece mayor velocidad en la transimisión de información más compleja como puede ser el envío y procesado de vídeos; y la tecnología digital para móviles GPRS/GSM (General Packet Radio Service/Global System for Mobile communications), utilizada por los teléfonos móviles de segunda generación (2.5G y 2G).

Por último hemos querido incluir las Redes del Mundo Virtual (Realidad Aumentada), en las cuales los usuarios interaccionan con un entorno artificial que puede estar o no inspirado en el mundo real. En este tipo de entornos virtuales, se establece una comunicación teórica entre agentes. La red de comunicación se realiza con todos los elementos presentes en el entorno virtual, sin límites teóricos en los que la distancia considerada es el universo. Dentro de estos entornos, se encuentran las aplicaciones desarrolladas en computación afectiva en los entornos relacionados con la salud, que ayudan a crear un entorno amigable para el usuario en la realización de pruebas médicas.

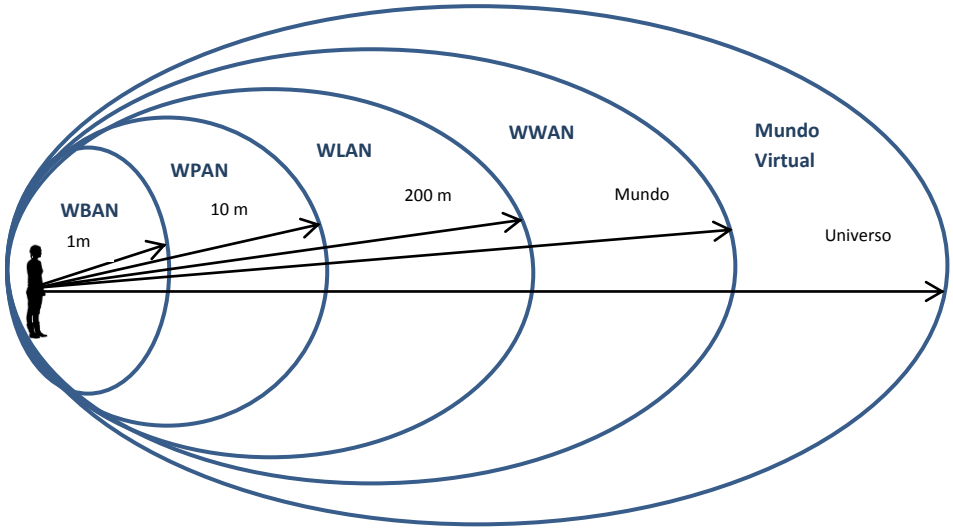

Figura 3.10. Modelo general de redes inalámbricas según su alcance de cobertura

Entre los principales protocolos de comunicación de redes inalámbricas que más se utilizan en las aplicaciones del AmI estudiadas, tenemos los siguientes: NFC (WBAN), Bluetooth (WPAN), RFID y WiFi (WLAN), 3G/UMTS/GPRS/GSM (WWAN):

- La tecnología NFC (Near Field Communication) se caracteriza por trabajar a corta distancia, con frecuencias altas de comunicación. Se basa en un rango pequeño de conectividad inalámbrica que permite la comunicación de diferentes dispositivos cuando están muy próximos. Esta tecnología presenta un coste bajo y es compatible con el estándar internacional (ISO14443). Muchos de los teléfonos móviles actuales disponen de esta tecnología de comunicación parecida a la RFID, cuya principal diferencia es el pequeño rango de operación que suele ser menor de 4 cm. Para utilizar este tipo de tecnología, el usuario no necesita realizar ninguna configuración de emparejamiento con ningún dispositivo, como sí lo requiere la tecnología por Bluetooth. Con el simple contacto o toque con un dispositivo provisto de tecnología NFC, el usuario puede interactuar con los diferentes dispositivos del entorno y acceder a los diferentes servicios ofrecidos por éstos.

Las etiquetas NFC son lo suficientemente pequeñas (0,5 mm²) y presentan buena capacidad de memoria (hasta 1 Megabyte), lo cual les permite ser integradas en objetos tan comunes como teléfonos móviles, relojes, pulseras, tarjetas, etc., utilizándose, tanto para identificar al usuario, como para realizar pagos o transferir información, por lo que resulta muy útil en los dominios de aplicación del AmI. Así, encontramos este tipo de tecnología en operaciones de emisión de billetes, en la entrega/envío de conformidad de contenidos, así como en dispositivos para el control de accesos *[Laukkanen, M. 2007], [Geven, A. et al. 2007]*.

Figura 3.11. Aplicaciones de la tecnología NFC

- El estándar de comunicación inalámbrica Bluetooth para la transmisión de información, es uno de los más extendidos actualmente dentro de las redes de área personal, gracias a su bajo coste. Este tipo de estándar requiere la sincronización y configuración de los dispositivos que hay que comunicar. Gran parte de las aplicaciones del AmI en las que los servicios ofrecidos al usuario se realizan a través del teléfono móvil, emplean la tecnología Bluetooth como medio para transferir la información. En este punto, es importante destacar la conveniencia de no tener activo de forma permanente la conectividad por Bluetooth de los teléfonos móviles, ya que éstos pueden conectarse con otros equipos en cualquier momento, aumentando así la posibilidad de que puedan producirse ataques como por ejemplo el envío de malware a través de esta conexión.

Figura 3.12. Dispositivos con tecnología Bluetooth

- Los Sistemas RFID (Radio Frequency IDentification) proporcionan capacidad de comunicación con identificación única entre el lector (receptor) y el objeto donde se encuentra insertada la tarjeta RFID (emisor), sin necesidad de contacto, ni de línea de visión directa entre ambos dispositivos. Dentro de las redes inalámbricas de área local, destaca como una de las tecnologías más utilizadas en gran parte de los dominios de aplicación del AmI, como el hogar, el cuidado de la salud, el ocio y entretenimiento. Las tecnologías RFID y NFC aparecen en muchas de las aplicaciones del AmI, sobre todo en las desarrolladas en los dominios del cuidado de la salud y del AAL (Ambient Assisted Living) *[Lahtela, A. et al. 2008]*, *[Bravo, J. et al. 2008]*.

  El bajo coste de estas etiquetas y la reducción de su tamaño, permite su incorporación en casi cualquier objeto mediante la forma de etiquetas adhesivas (tamaño de hasta 0,4 mm^2). Estas etiquetas o tags permiten almacenar y enviar información a un lector a través de la emisión de ondas de radio. Las etiquetas RFID constan de una antena que se activa al inducir en ella una señal de radiofrecuencia (se encarga de transmitir la información que identifica a la etiqueta, un transductor (convierte la información transmitida por la antena en datos), y un microprocesador o chip (posee memoria interna para almacenar el número de identificación de la etiqueta y en algunos casos datos adicionales).

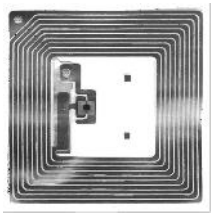

Figura 3.13. Etiqueta RFID

Los componentes que participan en la tecnología RFID son: las etiquetas, los lectores, el software que procesa la información y los programadores.

Las etiquetas RFID pueden ser de tres tipos: pasivas (sin fuente de alimentación, alcance hasta 10 cm), semipasivas (con fuente de alimentación del microchip) y activas (con fuente de alimentación para la transmisión de señales, alcance de 500 m, y en algunos casos varios kilómetros).

Figura 3.14. Tipos de etiquetas RFID. De izda. a dcha.: Pasiva, Activa

Los lectores RFID reciben la información emitida por las etiquetas y la transfieren al subsistema de procesamiento de datos o middleware. El lector consta de tres partes: antena, transceptor, y decodificador. Algunos lectores incorporan un módulo programador que les permite escribir información en las etiquetas, si éstas permiten la escritura. El subsistema de procesamiento de datos o middleware, es un software que reside en un servidor, sirviendo de intermediario entre el lector y las aplicaciones, y que se encarga de filtrar los datos que recibe del lector o red de lectores.

Los programadores RFID son los dispositivos encargados de realizar la escritura de información sobre la etiqueta RFID, es decir, codifican la información en un microchip alojado dentro de la etiqueta (esta programación puede realizarse en una sola vez única, si las etiquetas son sólo de lectura, o en varias veces, si las etiquetas son de lectura/escritura).

La regulación del sistema de asignación de códigos RFID a entidades y empresas se lleva a cabo por la organización mundial EPC Global (Electronic Product Code) que asigna el Código Electrónico de Producto único para identificar de manera exclusiva cualquier objeto a nivel mundial (longitud de 24 dígitos hexadecimales). Por otra parte, la International Organization for Standarization (ISO) establece las normas sobre este tipo de tecnología para su estandarización, estableciendo los requisitos reguladores a nivel mundial, aunque cada país regula las frecuencias permitidas, las emisiones y otras características de funcionamiento, por lo que los estándares actuales no son interoperables al cien por cien entre sí, ni con otras tecnologías.

La tecnología RFID por sí misma genera importantes amenazas a la privacidad y el anonimato de los individuos debido, fundamentalmente, a que las etiquetas RFID, pueden ser empleadas para la identificación del portador o sus pertenencias, por parte de terceros lectores sin el consentimiento previo del propietario. Este filtrado de información puede conducir a actividades de seguimiento de la localización o creación de perfiles del usuario. Por ello, la utilización de este tipo de tecnología requiere adoptar medidas de seguridad específicas que proporcionen los niveles de privacidad y seguridad adecuados para el usuario, de tal forma que garanticen que la comunicación e identificación del mismo, se lleva a cabo únicamente por los dispositivos autorizados en el contexto de la red en la que se encuentre el usuario.

- La tecnología WiFi (Wireless Fidelity) es una de las redes inalámbricas de área local (WLAN) más extendida y utilizada en la actualidad, estando presente en la mayoría de los entornos en los que nos encontramos de manera habitual, ya sea a través de un router propio o de una red WiFi pública (la gran mayoría de las conexiones a Internet de los hogares españoles es a través de una red inalámbrica WiFi). El alcance medio de este tipo de tecnología está en 150 m, llegando a alcanzar los 200 m. Ofrece una buena velocidad y flexibilidad en la transmisión de la información, presentando un estándar consolidado (IEEE 802.11). Uno de los estándares más seguros para la protección de las conexiones WiFi en el hogar es el WPA o WPA2.

Figura 3.15. Dispositivos conectados por WiFi

- Las redes de área ampliada UMTS (3G/4G/5G)/GPRS/GSM permiten la movilidad del usuario, dando soporte a la comunicación inalámbrica en áreas extensas de cualquier parte del mundo, gracias a la utilización de los teléfonos móviles. Mediante la asignación de canales de frecuencia de radio, este tipo de tecnología digital ofrece al usuario una gran disponibilidad tanto para el envío, como para la recepción de datos a través del teléfono móvil. Los teléfonos móviles que utilizan el estándar de comunicación GSM son también conocidos como de segunda generación (2G), permiten una descarga de datos digital de unos 100 kbps, presentando el inconveniente de desconectarse cuando no hay cobertura, por lo que muchas veces se ralentizan los procesos de descarga de

contenidos web, videoconferencias, etc. El estándar GPRS se basa en una optimización del GSM, orientada exclusivamente a la transmisión de datos mediante telefonía móvil, se conoce también como 2.5G. Los teléfonos móviles actuales que utilizan las redes UMTS (móviles de tercera y cuarta generación, 3G/4G), ofrecen mayor rapidez y prestaciones en el envío y recepción de la información, sobre todo en el envío y procesado de vídeos. La siguiente generación de redes móviles, las redes 5G que se podrán utilizar en el 2020 permitirán miles de millones de conexión a Internet a una velocidad nunca vista, y permitirá no solo ser utilizada en los teléfonos móviles sino que servirá también para llevar la conectividad a una gran cantidad de dispositivos en el llamado Internet de las cosas.

La mayoría de los operadores y teléfonos móviles permiten el uso dual de este tipo de redes, por lo que podemos disponer de la cobertura que exista, según el lugar en el que nos encontremos.

Figura 3.16. Dispositivos conectados por redes móviles

3.5.3. Interfaces de usuario multimodales

Las interfaces de usuario multimodales constituyen una de las tecnologías esenciales en los sistemas desarrollados en los dominios de aplicación del AmI, ya que son las que permiten la interacción del usuario con los servicios ofrecidos en los entornos inteligentes, sirviendo de puente entre el mundo físico y el mundo digital *[B. Ullmer and H. Ishii, 2001]*.

Estas interfaces deben ofrecer al usuario el soporte adecuado para que su interacción con las aplicaciones desarrolladas en AmI tenga lugar de la manera más sencilla y natural posible, adaptándose a las necesidades y requerimientos de los usuarios. Las interfaces de usuario utilizadas en los entornos inteligentes han de tener capacidad para analizar las entradas que recibe y generar las salidas de la forma más adecuada posible, según el contexto en el que se encuentre el usuario *[Maybury, M. 1999]*. Se puede decir que las interfaces de usuario son la forma (imagen, texto, sonido, etc.) en la que el usuario percibe la aplicación con la que interacciona, y la manera en la que el usuario establece la comunicación con el sistema en el que se encuentra desarrollada la aplicación.

En la última década, los avances en el procesado de audio, voz y lenguaje humano, el reconocimiento de formas, la visión por computador y la robótica han hecho posible el desarrollo de estas tecnologías interactivas multimodales, estando presentes en gran parte de los dominios de aplicación del AmI, proporcionando diversos servicios a los usuarios como: subtítulos de programas de televisión, transcripciones de programas de radio a personas con discapacidad auditiva, búsquedas, recuperación y transcripciones de imágenes, texto, música y contenidos multimedia, transcripción de conferencias y sesiones judiciales, reconocimiento de caras, seguimiento de personas y reconocimiento de actividad humana, diagnósticos médicos, análisis de la estructura de documentos, sistemas avanzados de asistencia a la conducción de vehículos, robótica ubicua, sistemas de diálogo multimodales, etc.

Las interfaces de usuario multimodales utilizadas en los dominios de aplicación del AmI, presentan la capacidad de comunicarse con el usuario mediante distintos canales de comunicación, como pueden ser el habla, los mensajes escritos, los gestos, etc. Estas interfaces inteligentes se encuentran presentes en las aplicaciones del AmI con las que el usuario interacciona a través de dispositivos como: Ordenadores personales, PDA (Personal Digital Assistant), Tablet, Smartphone, TV multimedia, Smart Objects, Wereable computers, Consolas de videojuegos, Realidad aumentada, etc.

Figura 3.17. Diferentes desarrollos de interfaces de usuario

3.5.4. Plataformas inteligentes (Agentes y Sistemas Multiagente)

Hasta ahora, hemos visto las principales tecnologías utilizadas en las aplicaciones del AmI que componen los sistemas para desarrollar la visión de la Inteligencia Ambiental: dispositivos de computación ubicua (Sensores inteligentes), comunicaciones ubicuas (Redes de comunicación inalámbrica), e Interfaces de usuario multimodales (Capítulo 1, Introducción). En la creación de los entornos inteligentes, resulta necesario integrar todas estas tecnologías en una plataforma inteligente distribuida que sea sensible al contexto en el que se encuentra el usuario.

Esta plataforma inteligente será la encargada de recibir la información (tanto del usuario como del contexto en el que se encuentre) que ha sido adquirida por los sensores inteligentes, y transmitida a través de las redes de comunicación inalámbrica, para comunicarse con el usuario a través de las interfaces multimodales ofreciéndole, de esta forma, servicios personalizados. Entre las capacidades que debe presentar esta plataforma de integración sistema-usuario en los sistemas desarrollados en AmI, destacan las siguientes: reconocimiento, aprendizaje, adaptación, anticipación, respuesta, y/o actuación según la situación en la que se encuentre el usuario en un

determinado entorno, ofreciéndole los servicios que puedan resultarle más útiles en cada momento, y atendiendo a sus preferencias, requerimientos o necesidades.

Los Agentes Inteligentes son una de las herramientas que mejor se adaptan a las necesidades y características de esta plataforma inteligente distribuida ya que, gracias a sus capacidades de autonomía, reactividad, pro-actividad, habilidades sociales, razonamiento, aprendizaje, y movilidad entre otras, permiten desarrollar la visión de la Inteligencia Ambiental en la creación de los entornos inteligentes del AmI. Los Agentes Inteligentes permiten desarrollar sistemas con capacidades de computación y comunicación ubicua, que facilitan la integración e interacción (interfaz) del usuario con las tecnologías y dispositivos presentes en los entornos inteligentes desarrollados en AmI.

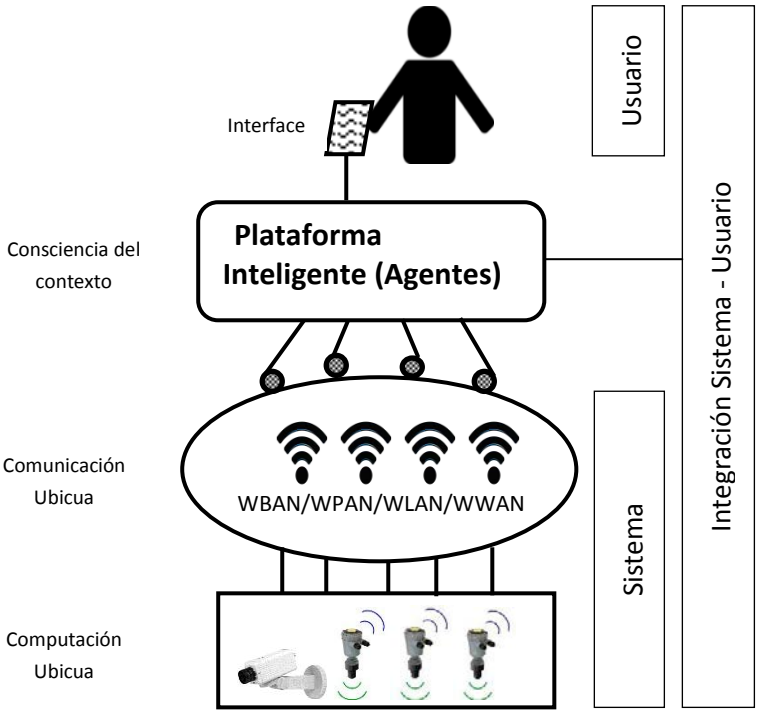

Figura 3.18. Arquitectura sistemas desarrollados en AmI

Los Agentes y Sistemas Multiagente son muy utilizados en los dominios de aplicación de la Inteligencia Ambiental, que por su naturaleza ubicua requiere una arquitectura de información y resolución de problemas distribuida, siendo conocidos como facilitadores de este tipo de arquitecturas, utilizándose en distintos niveles: para modelar dispositivos individuales presentes en un determinado dominio o entorno, para coordinar las actividades de las entidades (nivel middleware), o para formar la interface de usuario.

Los Agentes Inteligentes pueden ser considerados como una de las disciplinas más novedosas dentro del área de la Inteligencia Artificial, ya que permiten desarrollar sistemas que de manera autónoma son capaces de tomar decisiones y de coordinarse entre ellos. Gracias a la utilización de los Agentes Inteligentes, es posible abordar de una manera más eficaz la construcción de sistemas inteligentes complejos, con aplicación en campos tan diversos como son: la industria, la salud, el comercio electrónico, la educación, el entretenimiento, etc.

El concepto de Agente surge en los años 90 y, aunque existe una amplia variedad de definiciones sobre lo que es un Agente, no hay todavía una definición que esté aceptada universalmente. Entre estas definiciones, hemos destacado las siguientes:

- Agente es cualquier entidad que recibe entradas sensibles de su entorno, y a la vez es capaz de ejecutar acciones que pueden cambiar ese entorno. Se trata de un sistema (hardware o software) capaz de aprender de la experiencia, por lo que resulta razonable dotarle de ciertos conocimientos iniciales *[Russel, et al. 1995].*

- Los Agentes son sistemas computacionales que habitan en entornos dinámicos complejos, perciben y actúan de forma autónoma en ese entorno, realizando un conjunto de tareas, y cumpliendo los objetivos para los cuales han sido diseñados *[P. Maes 1995].*

- Un Agente es un sistema situado en alguna parte de un entorno, que percibe dicho entorno y actúa en él en beneficio de sus propias metas; el efecto de su actuación se nota en el entorno *[Franklin, S. et al. 1996]*.

- Los Agentes son entidades que colaboran con los usuarios mejorando la realización de sus tareas *[Foner, L.N. 1993]*.

- Un Agente es una entidad formada por estados o componentes mentales (como los que tienen las personas), como creencias, capacidades, elecciones, y compromisos. Dichos estados determinan las acciones que llevan a cabo los agentes, que se encuentran afectadas por los mensajes que reciben *[Shoham, Y. 1993]*.

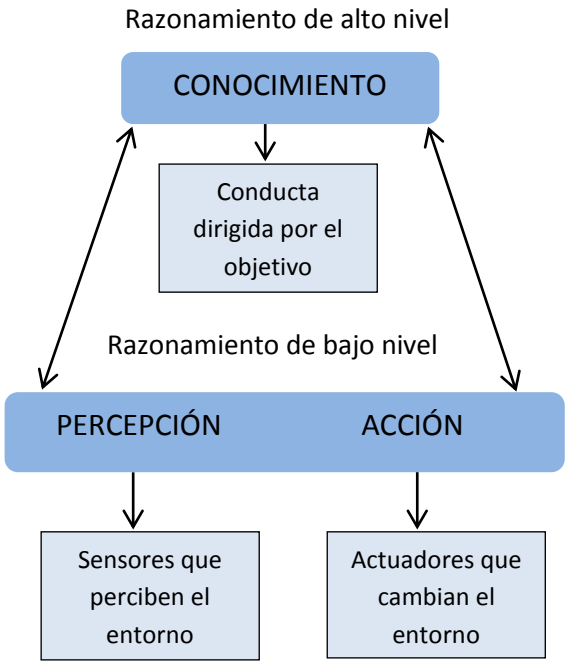

Figura 3.19. Conceptualización de Agente

En *[N. R. Jennings and M. Wooldridge, 1998]* se describe a los Agentes Inteligentes como el nuevo paradigma en el desarrollo de los sistemas software, presentando una de las definiciones más extendida sobre el concepto de Agente en la que se define a un Agente como un sistema informático situado en un entorno que presenta la capacidad de realizar acciones de manera autónoma, para conseguir los objetivos para los que ha sido diseñado.

Todas estas definiciones pueden resumirse diciendo que un Agente es una entidad interactiva y autónoma (software y/o hardware), con capacidades para percibir el entorno y actuar sobre él de una manera inteligente, dando respuesta en el cumplimiento de sus objetivos, sin necesitar de la intervención continua y/o directa del usuario. Es decir, son entidades (sistemas) que perciben y actúan sobre un determinado entorno.

Aunque las definiciones del concepto de Agente son diversas, es posible determinar algunas de las propiedades más notables que caracterizan a los Agentes *[J.M. Corchado and J.M. Molina, 2001]*:

- Autonomía: los Agentes presentan la capacidad de actuar sin la intervención directa de personas, disponiendo de control sobre sus actuaciones y estado interno. Su conducta viene definida por su propia experiencia que les permite aprender y mejorar.

- Adaptabilidad: son capaces de tomar decisiones acordes a los cambios producidos en el entorno.

- Razonamiento: un Agente tiene unos objetivos específicos que siempre intenta llevar a cabo (los cuales no deben ser contradictorios) y, en base a ellos, puede modificar su comportamiento.

- Sociabilidad: capacidad para interactuar mediante la comunicación con otros agentes, que pueden ser humanos.

- Reactividad: los Agentes perciben el entorno en el que se encuentran inmersos (Interfaz de usuario, conjunto de agentes, Internet, o todo esto combinado), respondiendo de manera rápida a los cambios producidos en dicho entorno.

- Iniciativa: los Agentes no actúan simplemente en respuesta a los cambios producidos en su entorno, sino que son capaces de mostrar comportamientos dirigidos a los objetivos que ha de satisfacer, tomando su propia iniciativa en un momento dado.

- Continuidad temporal: un Agente es un proceso que mantiene su identidad y estado en largos periodos de tiempo. Este proceso debe ser ejecutado de manera continua en el tiempo, desarrollando su función.

- Movilidad: capacidad de poder migrar a otra plataforma a través de una red telemática.

- Colaboración: han de ser capaces de trabajar en grupos para la consecución de un objetivo común.

- Personalidad: los Agentes contienen atributos que los caracterizan, mostrando su comportamiento más humano.

- Veracidad: propiedad por la que se asume que un Agente no comunica información falsa, al menos de manera intencionada.

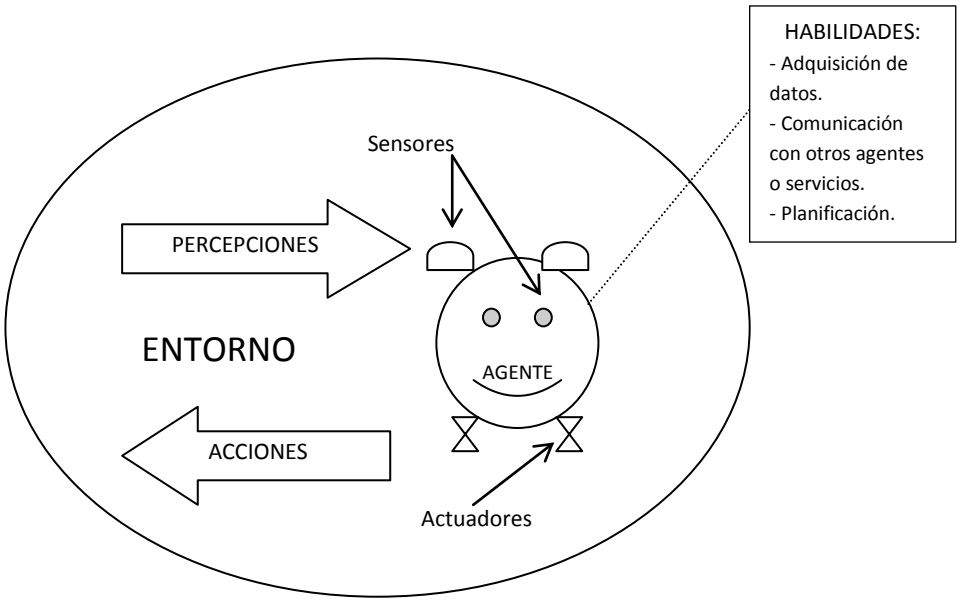

Figura 3.20. Esquema de Agente

Dependiendo de los roles asignados a los Agentes, en los diferentes entornos en los que se desarrollan, se identifican cuatro tipos básicos de Agentes, en orden creciente de generalidad *[Russell et al. 1995]*:

- *Agentes Reflejo Simple:* las reglas que los definen tienen la forma de condición/ acción (IF condición THEN acción). Primero se agrupan las reglas que perciben para especificar, después, la acción que tienen que tomar. Este tipo de Agentes suelen tener poco alcance.

- *Agentes Reflejo con Estado*: estos Agentes incluyen un tipo de estado interno, memoria, operando de forma que encuentran una regla cuya condición coincida con la situación del momento, procediendo así a realizar la acción correspondiente con dicha regla.

- *Agentes basados en Metas*: la consideración del concepto de meta ayudará al Agente a decidir cuáles son las acciones correctas, describiendo cuáles son las situaciones deseables en un determinado ambiente. Si la meta no es inmediata a una acción concreta, el Agente deberá realizar algún tipo de proceso de búsqueda y planificación que tendrá en cuenta la forma en la que cambia el ambiente donde se encuentra, para alcanzar su meta. Este tipo de Agente es muy flexible.

- *Agentes basados en Utilidades*: en estos Agentes las metas no resultan suficientes para generar un comportamiento de calidad, por lo que la consideración de la utilidad del Agente servirá para distinguir la preferencia entre un tipo de estado u otro. La utilidad mapea un estado a un número real. Este tipo de Agentes debe tener en cuenta las metas que puedan ser conflictivas y/o inciertas en la consecución del objetivo.

La arquitectura de un Agente define los mecanismos para interconectar tanto los diferentes componentes software como los dispositivos hardware, que permiten al Agente exhibir su comportamiento. Dado que existen multitud de áreas de aplicación de los Agentes, existen también infinidad de propuestas de arquitecturas particulares que especifican la manera de descomponer los módulos integrantes del sistema y su inter-operatividad, para lograr la funcionalidad requerida por el Agente. Así pues, uno de los aspectos básicos que diferencia una arquitectura de Agentes de otra, consiste en el método de descomposición del agente en tareas particulares. A continuación se presenta la clasificación de las arquitecturas de Agentes más extendida, en función del modelo de razonamiento utilizado, *[Wooldridge and Jennings, 1995]*:

- *Deliberativas*: utilizan modelos de representación simbólica del conocimiento y suelen estar basadas en la teoría clásica de planificación, se parte de un estado inicial, existe un conjunto de planes y un estado objetivo que se debe satisfacer *[Maes, P. 1989].* Un ejemplo de esta arquitectura lo constituyen los agentes intencionales, sistemas de planificación en los que se tiene en cuenta las creencias e intenciones, para definir los planes *[Jennings, N.R. 1993]*. Dentro de este tipo de arquitectura, destacan las basadas en el modelo BDI (Believes, Desires, Intentions) que constituye uno de los modelos más utilizados en la actualidad *[Rao, A.S., et al. 1995]*; el Agente utiliza sus creencias, deseos e intenciones para razonar.

- *Reactivas*: este tipo de arquitecturas se caracteriza por no tener como modelo central de razonamiento un modelo simbólico; suelen estar organizadas en jerarquías de tareas de menor a mayor nivel de abstracción (capas) que son las que definen el comportamiento del Agente *[Brooks, R.A. 1991].*

- *Híbridas:* en la construcción de este tipo de arquitectura se combinan aspectos de las arquitecturas deliberativas y de las reactivas. Las capas de organización de estas arquitecturas pueden estar estructuradas jerárquicamente de manera vertical (una única capa tiene accesos a los sensores y actuadores), o de forma horizontal (todas las capas tienen acceso a los sensores y actuadores). El comportamiento global del agente viene definido por la interacción entre tres niveles principalmente: reactivo (nivel más bajo), conocimiento (nivel intermedio), social (capa de más alto nivel). Ejemplos de estas arquitecturas son TouringMachines (Ferguson 1992) e Interrap (Müller 1997).

La mayoría de las aplicaciones de Agentes desarrolladas en Inteligencia Ambiental utilizan arquitecturas deliberativas del modelo BDI (Believes, Desires and Intentions). En este tipo de sistemas, los Agentes presentan capacidades de computación y utilizan un modelo de razonamiento basado en experiencias reales, que les permite realizar una gestión de la memoria y una planificación de las acciones más idóneas, para la consecución del objetivo.

En general, se puede considerar que los Agentes no son desarrollados de forma independiente, sino que, se desarrollan como entidades integradas en un sistema distribuido. A este sistema se le denomina Sistema Multiagente *[Huhns, M.N., et al. 1998]*, MAS (MultiAgent Systems). Este conjunto de Agentes ha de tener capacidad para cooperar, coordinar y negociar, por lo que los diferentes agentes integrantes del sistema deben interactuar entre ellos. Estos Sistemas Multi-Agentes han de coordinar, de manera inteligente, el conjunto de Agentes autónomos, organizando sus conocimientos, metas, propiedades y planes para la toma de decisiones que resulte más acorde con la consecución de su objetivo o la resolución de un problema. En *[Corchado, J.M. et al. 2008]* se presenta una arquitectura Multiagente para el desarrollo de servicios distribuidos.

Las interacciones más habituales que se realizan en los MAS, como son informar o consultar con otros agentes (“hablar” entre ellos), les permite tener en cuenta lo que realiza cada uno de ellos, así como razonar sobre el papel que desarrolla cada agente dentro del sistema. Esta comunicación entre agentes se realiza por medio de un lenguaje de comunicación de agentes llamado ACL (Agent Communication Language). Otro de los estándares utilizados para la comunicación ente agentes heterogéneos es FIPA (Foundation for Intelligent Physical Agents), en el que se definen las normas para implementar sistemas basados en agentes (plataformas de agentes), y se especifican la forma en la que éstos se comunican e interactúan.

Las aplicaciones basadas en el desarrollo de Agentes y Sistemas Multi-Agentes vienen siendo utilizadas en infinidad de áreas desde hace tiempo, pudiéndose agrupar éstas en los siguientes dominios de aplicación: aplicaciones industriales, aplicaciones comerciales, aplicaciones médicas, y aplicaciones de entretenimiento.

- Aplicaciones industriales**.** La utilización de Agentes resulta muy apropiada en el desarrollo de sistemas distribuidos presentes en este tipo de aplicaciones. Dentro de esta línea, se pueden destacar las aplicaciones que se encargan de:

- Control de procesos: los controladores son por sí mismos sistemas reactivos. Se puede destacar la gestión autónoma de edificios inteligentes desde el punto de vista de la seguridad y del control de recursos; la gestión del transporte de electricidad; la monitorización y control de fallos en plantas industriales; el control del tráfico aéreo, etc.

- Control de la producción: planificación y agenda de la producción o fabricación de productos. Sistemas encargados de las fases de ensamblaje, pintado, almacenamiento de productos, control de existencias, etc.

- Aplicaciones comerciales: las más utilizadas son a nivel de red, tanto en Internet como en redes corporativas, destacando las siguientes:

- Gestión de la Información: recopilación automática de la información disponible en la red, filtrado inteligente del correo electrónico, de grupos de noticias, planificación de la agenda personal.

- Comercio electrónico: proporciona el entorno virtual donde poder realizar operaciones comerciales o tareas de búsqueda de productos, de manera automatizada.

- Monitorización: ofrece al usuario la información cuando ocurre un determinado acontecimiento, como puede ser que la información se ha actualizado, se ha trasladado de lugar o que ha sido borrada. Este tipo de Agentes alerta al usuario frente a eventos en la red que pueden resultarle de gran utilidad.

- Mediador entre diferentes fuentes de información: los Agentes que hay que desarrollar han de permitir la inter-operatividad con las diferentes fuentes de información disponibles, independientemente del sistema en el que se hayan desarrollado.

- Aplicaciones médicas: la idea en este tipo de aplicaciones es la de disponer de Agentes que realicen de forma autónoma tareas que puedan ser automatizadas en un hospital, como por ejemplo:
- Monitorización: control de los pacientes ingresados en determinadas áreas hospitalarias (unidades de cuidados intensivos), en una residencia, etc.

- Atención al paciente: sistemas para el seguimiento del tratamiento de un paciente según su enfermedad.

- Aplicaciones de Entretenimiento: entre las aplicaciones desarrolladas en este domino tenemos:
- Juegos: mediante el desarrollo de Agentes en este entorno se pueden crear juegos más sofisticados con características inteligentes, donde se pueden incorporar personajes virtuales que pueden incluso funcionar de forma autónoma.

- Teatro y Cine interactivo: el usuario puede interpretar el papel de un personaje dentro de una obra de teatro o película de cine, siendo el resto de los personajes virtuales.

A continuación se citan algunos de los Sistemas Multiagente desarrollados en los dominios de aplicación del AmI: sistemas para la asistencia de las personas mayores *[K. Z. Haigh, et al. 2002], [A. Muñoz, et al. 2001]*; sistema de asistencia a los visitantes de un museo, *[Bombara et al. 2003]*; sistema para que los usuarios soliciten un servicio de taxi *[Moreno et al. 2003]*; sistema de asistencia al usurario en un laboratorio *[Susperregi et al. 2004]*; sistema para la monitorización de pacientes con Alzheimer en una residencia geriátrica *[Corchado et al. 2008]*; asistente personal para la realización de viajes *[Spanoudakis and Moraitis, 2006]*; sistema para la asistencia y el cuidado en el hogar *[Fraile, J.A. et al. 2008]*; sistemas para el aprendizaje *[W.L. Johnson, et al. 2000]*, *[Mbala and A.G.N. Anyouzoa, 2005]*; sistema para rehabilitación de niños con autismo *[K. Sehaba and P. Estraillier, 2005]*; sistema de vigilancia con multi-sensores *[J. Pavón, et al. 2007]*.

Entre los beneficios aportados por el uso de los Agentes Inteligentes en el desarrollo de las aplicaciones del AmI, destacan los siguientes *[J.M. Corchado and J.M. Molina, 2001]*: facilitan la realización de tareas al usuario, actúan como consultores, sirven de operadores en medios complejos, actúan de manera satisfactoria en una amplia variedad de entornos. Todo ello, gracias a los procesos que son capaces de ser desarrollados por los Agentes entre los que se encuentran: la automatización (uso o comportamiento repetido por parte del usuario), la personalización (el Agente puede presentar la información adecuada que se adapta a los usos personales y al estilo de interacción que prefiere el usuario), la notificación (el Agente puede dar servicios de notificación al usuario, como notificaciones que le protejan de recibir información no deseada, o notificaciones de la existencia de dispositivos de acceso a su información, etc.), el aprendizaje (el Agente aprende la realización de tareas que pueden automatizarse, o aprender preferencias que pueden usarse para personalizar el agente), y la tutorización (el Agente puede actuar como guía para el usuario, gracias a su control sobre los eventos producidos).

Las capacidades de autonomía, pro-actividad, habilidades sociales, razonamiento, aprendizaje, coordinación, y adaptabilidad de los Agentes Inteligentes, entre otras, facilitan el desarrollo de los entornos inteligentes del AmI, permitiendo la gestión inteligente de la información de manera autónoma, adaptándose a las necesidades del entorno en el que se encuentran y permitiendo la escalabilidad del sistema desarrollado.

3.6. CONCLUSIONES

El importante incremento en el número de contribuciones e investigaciones desarrolladas en los últimos 15 años, dentro del área de las aplicaciones de la Inteligencia Ambiental, nos ha permitido llevar a cabo una revisión de las mismas que nos ha permitido, por un lado, identificar cuáles son las mejoras necesarias en el desarrollo del AmI, y, por otro, buscar otras posibles áreas de investigación, que nos ayudarán a consolidar y aumentar su potencial de aplicación, así como su aceptación por parte de los usuarios. Entre las características más notables que deben considerarse en el desarrollo de la Inteligencia Ambiental para su verdadera integración y aceptación social, destacamos las siguientes:

- Mejorar el contacto con las personas.
- Estar orientadas hacia la mejora de la comunidad y de la cultura en general.
- Ayudar a mejorar el conocimiento y desarrollo de habilidades en ámbitos como el trabajo, las relaciones sociales, comerciales, etc.
- Inspirar confianza y seguridad.
- Ser sostenibles a largo plazo con el aprendizaje, proporcionando un entorno en el que la convivencia con los dispositivos existentes, resulte fácil.

- La manipulación y control de los entornos inteligentes desarrollados debe poder ser controlable por el público en general, en lo que se refiere a la forma en la que adquieren y transmiten la información personal.

En base al estudio realizado sobre los dominios de aplicación del AmI, y las tecnologías utilizadas, en la siguiente figura indicamos los aspectos tecnológicos y sociales más relevantes de las aplicaciones desarrolladas en Inteligencia Ambiental:

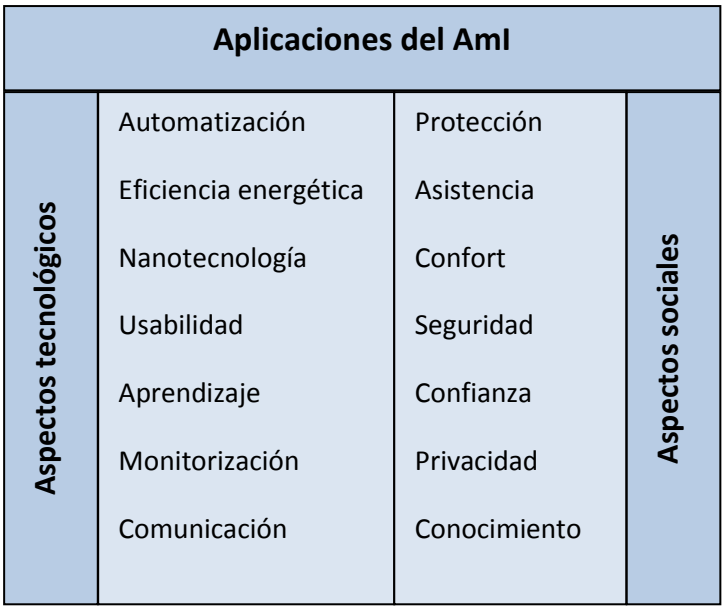

Figura 3.21. Aspectos socio-tecnológicos de las aplicaciones del AmI

Según la visión desarrollada por la Inteligencia Ambiental, el ser humano se sitúa en el centro del desarrollo actual y futuro de las Tecnologías de la Información y la Comunicación. Como hemos visto, es indiscutible el hecho de que el uso de este tipo de tecnologías en las aplicaciones desarrolladas en AmI nos ofrece grandes ventajas, al facilitarnos la realización de la mayoría de las actividades que realizamos a diario, a través de los servicios ofrecidos. Entre estas ventajas se encuentran las siguientes:

- Facilitar y permitir la comunicación.
- Aportar interactividad tanto a nivel técnico, como multimedia y social.
- Permitir la portabilidad gracias a su ubicuidad.

- Facilitar el acceso a una inmensa cantidad de servicios e información.
- Poseer gran capacidad de almacenamiento.

Pero también, poseen una serie de desventajas, obtenidas de la propia percepción y experiencia de los usuarios al interaccionar con las tecnologías y aplicaciones desarrolladas en Inteligencia Ambiental, que deben tenerse en cuenta, para inspirar confianza y conseguir así su verdadera aceptación por parte de éstos. Los inconvenientes más destacables son:

- La obsolescencia de los dispositivos computacionales, que limitan su capacidad de actualización para llevar a cabo su mantenimiento.
- La seguridad y confianza.
- La falta de privacidad.

Teniendo en cuenta todas estas cuestiones, para el verdadero desarrollo de la Inteligencia Ambiental en la creación de entornos inteligentes, resulta necesario mejorar una serie de cuestiones socio-tecnológicas, entre las que destacamos las siguientes:

- Los dispositivos de computación y los sensores inteligentes, encargados de la adquisición del contexto en el que se encuentra el usuario, han de tener un hardware miniaturizado, mediante el uso de la nanotecnología.
- Es necesario desarrollar una infraestructura de comunicación fija y/o móvil, en la que las redes de comunicación, tanto cableada como inalámbrica, sean capaces de converger e inter-operar.
- Las redes de los dispositivos han de ser dinámicas y deben estar distribuidas de forma masiva, sin necesidad de servidores centrales, con capacidad de cooperación.
- Las interfaces de usuario deben ser lo más natural y cercanas al ser humano.

- Sensibilidad al contexto. Nuestra localización, identidad o actividad han de servir como parámetros de entrada implícitos que permitan al entorno inteligente conocer la situación en la que nos encontramos, y así actuar en consecuencia.

- Software seguro y robusto que ofrezca confianza a los usuarios.

- Los diferentes dispositivos de computación y comunicación, deben minimizar los riesgos de invasión de nuestra privacidad.

La mayoría de las aplicaciones desarrolladas en los dominios de aplicación del AmI se encuentran dirigidas hacia la eliminación de las barreras existentes entre los usuarios y la tecnología utilizada. Estas barreras surgen como consecuencia de aspectos relacionados con cuestiones tan diversas como:

- La usabilidad
- El coste de los sistemas
- El ahorro energético
- La calidad del servicio
- La confianza
- La privacidad

A la hora de abordar estas cuestiones, conviene tener en cuenta que, uno de los aspectos más importantes que deben ofrecer los servicios desarrollados en las aplicaciones del AmI, es el de cubrir las necesidades reales de los usuarios para, de esta forma, aumentar su grado de aceptación y confianza. Entre estas necesidades, destacan las siguientes: el cuidado de la salud, la movilidad, la alimentación, la higiene, la memoria, el confort, los negocios, la educación, el ocio y entretenimiento, la seguridad, la privacidad, la salud emocional.

Para la integración de estas necesidades en el desarrollo de las aplicaciones del AmI, hay que tener en cuenta diferentes cuestiones como: la construcción de servicios que prevengan desajustes en las condiciones adecuadas, tanto a nivel ambiental (luz, calefacción, acústica, etc.), como a nivel del propio usuario (parámetros vitales, fisiológicos, etc.); focalizar al usuario como agente activo que participa en el desarrollo de las aplicaciones; desarrollo de interfaces sencillas, intuitivas y personalizadas, capaces de adaptarse a los usuarios tanto desde el punto de vista de sus necesidades, como de sus capacidades; aplicación de los servicios ofrecidos en diferentes contextos (las actividades cotidianas no son iguales en un contexto urbano que en uno rural); ofrecer servicios que inspiren confianza y seguridad al usuario.

Otro de los grandes retos de las aplicaciones desarrolladas en Inteligencia Ambiental es el relativo a la estandarización e integración de todos los componentes tecnológicos (Redes de sensores inalámbricos, sistemas embebidos, sistemas RFID, NFC, etc.), en una plataforma de sistemas inteligentes que, además de presentar la capacidad de alimentar contexto, personalizarlo, adaptarlo y anticiparse a los servicios requeridos por los usuarios, tenga también en cuenta las cuestiones sociales y éticas relativas tanto a la seguridad, como a la fiabilidad y privacidad de la información adquirida y transmitida. En este sentido, algunos de los problemas que resulta necesario abordar son:

- La existencia de múltiples fuentes de información (fusión).
- La sincronización temporal y la integración.
- Los mecanismos para enviar la información contextual a las aplicaciones.
- La utilización de un mismo dato contextual en diferentes aplicaciones.
- La inteligencia para procesar la información, deducir su significado y actuar en consecuencia.

En el desarrollo de las aplicaciones del AmI, no solo es importante la elección de la topología de la red de comunicaciones por la que se van a transmitir los datos, sino que resulta fundamental conseguir que dichos datos se transmitan de una manera fiable y segura, que garantice nuestra privacidad. Este punto resulta especialmente crítico en algunos dominios de aplicación del AmI, en los que el contenido de la información que se envía y recibe es altamente confidencial (datos médicos), por lo que las aplicaciones del AmI deberían diseñarse en base al dominio en el que se desarrollan. Otro problema con el que nos encontramos es el de la interoperabilidad de los datos. Aunque cada fabricante de soluciones desarrolladas en AmI, ofrece formatos/protocolos de comunicaciones privados y cerrados, para la captura y envío de los datos registrados, puede ocurrir que estos datos no solo se envíen a un sistema central, sino que también puede que sean consultados por terceros.

Las funcionalidades que ofrecen las redes de comunicación inalámbricas en los dominios de aplicación del AmI (movilidad y accesibilidad) también posibilitan la existencia de incidentes o ataques de seguridad, por lo que resulta imprescindible proteger dichas redes con unos protocolos de cifrado y estándares, evitando así que cualquier dispositivo que se encuentre en el radio de emisión pueda acceder a los datos que se están transmitiendo. La normalización en el ámbito de la tecnologías y dispositivos inalámbricos utilizados en las aplicaciones del AmI, como en cualquier otro ámbito tecnológico, resulta de vital importancia para disponer de unos servicios de calidad e interoperables, que ofrezcan seguridad en lo relativo a la protección de la privacidad de los datos adquiridos de los usuarios.

En el estudio de las aplicaciones desarrolladas en AmI, se observa que la mayoría de los desarrollos presentan una característica común, que es la necesidad de determinar la localización de los usuarios del sistema dentro del contexto en el que se encuentra. Esta localización es uno de los aspectos más importantes en el desarrollo de las aplicaciones del AmI, ya que permitirá al sistema determinar cuáles son los servicios más adecuados para el usuario según su ubicación, pero también supone un riesgo para la seguridad y protección de su privacidad.

Por otra parte, en los Entornos Inteligentes desarrollados por la Inteligencia Ambiental, las personas son también identificadas a través de diferentes dispositivos móviles de computación como: Smartphone, Tablet, Ordenadores Portátiles, Dispositivos de reconocimiento de imágenes por visión, Tarjetas de identificación (activas/pasivas), o incluso, por la actividad que realizan al acceder a los diferentes recursos que se encuentran disponibles en el entorno. Por ello, uno de los aspectos fundamentales que debe considerarse en el desarrollo de las aplicaciones del AmI, es el de ofrecer servicios seguros y fiables a través de los dispositivos computacionales y de comunicación, con el fin de minimizar los riesgos relativos a la privacidad de los datos de los usuarios, tanto en el momento de su adquisición como de su transmisión.

Como se ha indicado, las diferentes tecnologías utilizadas en los dominios de aplicación del AmI en su interacción con el usuario son capaces de adquirir y transmitir distintos tipos de información de éste, relacionada con su identidad, localización, actividad, gustos, orientación política, sexual, etc., por lo que resulta fundamental que, en el acceso a los servicios ofrecidos por las aplicaciones del AmI, se garantice la seguridad de esta información y se minimicen los riesgos relativos a la privacidad, impidiendo el acceso a la misma por terceras partes. En el diseño y desarrollo de las aplicaciones del AmI se necesita no solo abordar las cuestiones de tipo tecnológico, sino que resulta necesario también tener en cuenta las implicaciones sociales y éticas que se derivan del aumento en la adquisición y transmisión de la información extraída, tanto del propio usuario como de su actividad personal, por los dispositivos presentes en los dominios del AmI.

Resulta importante destacar que las tecnologías y dispositivos presentes en los dominios de aplicación del AmI han de ser conocidos por el usuario. Estas tecnologías utilizadas no deben ser invisibles para el usuario (visión original de la computación ubicua), sino que deben ser transparentes (el usuario ha de saber que están presentes). El usuario ha de saber de su existencia, conocer su naturaleza, y forma de actuación.

Este tipo de tecnologías deben también ofrecer al usuario la posibilidad de desactivarlas o inhibirlas, en algún momento o situación que requiera la más absoluta confidencialidad; y lo que es más importante, no deben transmitir la información adquirida a terceras partes, sin el conocimiento y consentimiento del usuario.

El éxito y aceptación de las aplicaciones desarrolladas en AmI depende en gran medida de la seguridad y el grado de confianza que nos muestren y de la forma en la que percibamos que no invaden nuestra intimidad. Las aplicaciones desarrolladas en los dominios del AmI deben utilizar tecnologías que susciten tranquilidad a los usuarios. Una herramienta útil para alcanzar estos objetivos es la utilización de los Agentes y Sistemas Multiagente, presentes en muchos de los dominios de aplicación del AmI que, gracias a sus capacidades de autonomía, habilidades sociales comunicación, razonamiento, aprendizaje, y planificación, permiten desarrollar la visión de la Inteligencia Ambiental de ofrecer servicios personalizados, ayudándonos a minimizar los riesgos de privacidad de nuestra información.

Capítulo 4

La privacidad en AmI

4.1. CONCEPTO DE PRIVACIDAD

La palabra privacidad se encuentra definida en el Diccionario de la Real Academia de la Lengua Española (DRAE) como el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". El término de lo que es "algo privado", es definido en el DRAE como "lo que se ejecuta a la vista de pocos, lo que es particular y personal de cada individuo, lo que no es de propiedad pública o estatal, sino que pertenece a particulares. En el Diccionario de uso del español actual Clave, se define la privacidad como "propiedad de lo que pertenece a la intimidad o a la vida privada de una persona". Por otra parte, según el Diccionario de uso del español María Moliner, la privacidad es definida como "la cualidad o condición de privado".

Conforme a estas definiciones, el concepto de la privacidad puede ser considerado como una dimensión del ser humano que es objeto de protección jurídica. Es decir, la privacidad es el derecho y propiedad a la propia intimidad y vida privada.

Teniendo en cuenta todas estas consideraciones, podemos decir que la privacidad es aquello que una persona realiza en un ámbito reservado, y que tiene derecho a mantener fuera del alcance de terceros, asegurándose la confidencialidad de sus temas privados. En este sentido, la privacidad se refiere a todos aquellos aspectos de la vida de un individuo que pertenecen a la esfera de lo personal, como son sus relaciones sentimentales y familiares, sus aficiones personales, sus bienes particulares, sus espacios físicos particulares, así como sus creencias en materia religiosa, política o ideológica.

De forma generalizada, la idea de la privacidad suele asociarse al concepto de intimidad que engloba las acciones, preferencias y sentimientos que no deben trascender fuera del ámbito íntimo o personal. Aunque resulta difícil establecer con precisión cuáles son los límites de la privacidad o intimidad, ya que éstos dependen de diversos factores y circunstancias, resulta importante destacar que el derecho a la intimidad se encuentra protegido por la ley.

A continuación, se describen algunos de los términos definidos legalmente que aparecen en este estudio, y que se encuentran vinculados al concepto de privacidad:

- *Información o Datos personales*: información relacionada con un individuo (proporcionado por él de manera consciente, o no), que permite poder identificarle personalmente. Entre esta información se encuentran los datos relacionados con su nombre, dirección de correo electrónico, información bancaria, etc.

- *Información o Datos confidenciales*: cualquier información personal sensible relacionada con temas como el origen étnico o raza, las creencias religiosas, la orientación sexual, la ideología política, los datos relacionados con la salud, etc.

- *Controlador de datos*: es el sistema que, de acuerdo con la legislación vigente, tiene competencias para determinar los contenidos y el uso de los datos personales, con independencia de si es él o un agente en su nombre el que los adquiere, almacena, procesa o divulga.

- *Flujo transfronterizo de datos personales*: referido al movimiento de los datos personales a través de fronteras nacionales.

La privacidad se encuentra inmersa en un amplio abanico de situaciones recogidas en los textos legales, presentando diferentes facetas que tienen conceptos relacionados entre sí, y que pueden ser clasificadas en:

- *Privacidad de la información*: bajo esta denominación se incluye el establecimiento de reglas que gobiernan la recolección y gestión de datos personales tales como información crediticia, así como registros médicos y gubernamentales. Se conoce también como "*protección de datos*".

- *Privacidad corporal*: este concepto hace referencia a la protección física de las personas ante procedimientos invasivos tales como pruebas genéticas, pruebas de drogas y registro de cavidades.

- *Privacidad de las comunicaciones*: esta faceta de la privacidad se refiere a la seguridad y privacidad del correo postal, llamadas telefónicas, correo electrónico y otras formas de comunicación como Internet, las redes sociales, el cloud computing, etc.

- *Privacidad territorial*: Este concepto hace referencia a la fijación de límites a la intromisión en los medios domésticos y otros, como pueden ser el centro laboral o espacios públicos. En esta categoría se incluyen los allanamientos, los sistemas de video-vigilancia, y los sistemas de control de identificación.

4.2. EL DERECHO A LA PRIVACIDAD

El derecho a la privacidad forma parte de la Declaración Universal de los Derechos Humanos 10/12/1948 (Artículo 12): "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. Esto significa que la privacidad es un derecho inherente al ser humano que con independencia de otros factores, no puede ser transferido ni puede renunciarse a él. El objetivo del derecho a la privacidad es el de garantizar la dignidad del individuo.

En los textos legales, la idea del derecho a la privacidad aparece bajo diferentes acepciones. Así, en la Constitución Española de 1978 esta idea aparece bajo el término "*intimidad"*. La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos (LORTAD) de 1992 introduce el término de la "*privacidad".* El Código Penal español de 1995, recoge la expresión "*delitos contra la intimidad"*. En el texto de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) de 1999, se dice que su finalidad es proteger la "*intimidad personal y familiar"*, y en la página *web* del Ministerio de Justicia español, en el epígrafe donde se anuncia dicha ley, se lee que la misma trata de ofrecer al ciudadano mayores garantías para la protección de su "*privacidad"*.

En nuestro país, la intimidad está considerada como un derecho fundamental y así aparece recogido en el Artículo 18 de la *Constitución Española de 1978*, donde queda constancia de aspectos tan importantes como:

- Que se encuentra garantizado, salvo que exista una resolución judicial contraria, el secreto de las comunicaciones (telefónicas, de correo postal, telegráficas, etc.)

- Que la intimidad es un derecho inviolable y que, como tal, está garantizado por la norma jurídica del Estado.

- Que la legislación existente en el país se encargará, entre otras muchas cosas, de limitar, en la medida que sea necesario, el uso de la informática para que no se puedan vulnerar la intimidad o incluso el honor.

En el *Código Penal Español, Ley Orgánica 10/1995 de 26 de noviembre*, quedan especificados los delitos contra la intimidad. Así, en los Artículos 169, 170 y 171 se regulan las amenazas que pueden ser constitutivas de delito. Se considera que una persona comete delito de amenazas cuando anuncie o advierta a otra con causarle un daño a él, a su familia o a otras personas con las que esté íntimamente vinculado. En el Título X sobre los Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, se regulan varios delitos que protegen la voluntad de una persona para que una determinada información o hecho no sean difundidos más allá de su propia intimidad o círculo cerrado. Esto pone de manifiesto el derecho que tienen las personas para controlar toda información o hecho que afecten a su vida privada y, por tanto, a su intimidad.

El derecho a la intimidad se configura como uno de los derechos de las personas más sutiles y más difíciles de delimitar y proteger por el Derecho Penal. Para tener una idea más clara sobre este tipo de delitos contra la intimidad recogidos en el Código Penal Español, Ley Orgánica 10/1995 de 26 de noviembre, presentamos los diversos tipos delictivos contemplados:

- Secretos documentales. Se castigará a aquél que se apodere de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales, en los que consten hechos que puedan calificarse como secretos o relativos a la intimidad de la persona.

- Interceptación de comunicaciones personales. La captación de cualquier comunicación oral solamente será castigada cuando se utilicen "instrumentos o artificios técnicos".

- Descubrimiento del secreto informático. Estará incurriendo en un delito de descubrimiento del secreto informático aquella persona que se apodere, utilice o modifique, sin estar autorizado y en perjuicio de tercero, "datos reservados de carácter personal o familiar" que se hallen registrados en ficheros, soportes informáticos, o en cualquier otro tipo de archivo o registro público o privado. Igualmente se castigará al que acceda por cualquier medio a los mismos, los altere o utilice en perjuicio del titular de los datos o de un tercero.

- Acceso a datos y sistemas informáticos. La regulación de este nuevo delito en el Código Penal pretende proteger a aquellas personas que han sufrido una intromisión de datos o programas informáticos por parte de un sujeto, que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accede o mantiene los mismos contra la voluntad de la persona que tiene el derecho a excluirlo.

- Revelación de secretos. La difusión de datos o hechos descubiertos o imágenes captadas ilícitamente por un sujeto suponen un mayor daño a la intimidad, y son castigadas con penas más duras que las conductas anteriores. Aquellas otras personas que revelen estos datos o imágenes sin haber tomado parte en su descubrimiento, pero sabiendo que la información revelada tiene un origen ilícito, serán castigadas igualmente, aunque con menor gravedad.

La *Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de carácter Personal (LOPD)* tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Entre otras disposiciones, destacamos las siguientes como las más relevantes que hay que considerar dentro del área de investigación de las aplicaciones del AmI:

- El derecho a la información en la recogida de datos: los interesados a los que se soliciten datos personales deberán ser previamente informados de modos expreso, preciso e inequívoco (Artículo 5).

- El consentimiento del afectado: el tratamiento de los datos personales requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa (Artículo 6).

- Datos especialmente protegidos (Artículo 7).

- Datos relativos a la salud (Artículo 8).

- La seguridad de los datos (Artículo 9): el responsable del fichero de almacenamiento de los datos, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnológica, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

- Comunicación de los datos (Artículo 11): los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

- Acceso a los datos por cuenta de terceros (Artículo 12).

- Título III, Derecho de las personas: Derecho de consulta (Artículo 14), Derecho de acceso (Artículo 15), Derecho de rectificación y cancelación (Artículo 16).

- Título IV, Disposiciones sectoriales: Ficheros de titularidad pública (Capítulo I): creación, modificación o supresión de ficheros (Artículo 20), Ficheros de titularidad privada (Capítulo II): Creación (Artículo 25), Comunicación de la cesión de datos (Artículo 27).

- Título V, Movimiento internacional de datos (Artículos 33 y 34).

- Título VI, Agencia de Protección de Datos (Artículo 35: Naturaleza y régimen jurídico, Artículo 37: Funciones).

El *Real Decreto 1720/2007 de 21 de diciembre que aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD)*, establece las medidas técnicas y de organización adecuadas que debe cumplir la empresa responsable del tratamiento de los datos personales de los usuarios registrados en un determinado sistema o aplicación, con el fin u objetivo de proteger la destrucción (accidental o ilícita), el mal uso, la alteración, la difusión, el acceso no autorizado y el robo de los datos facilitados por el usuario, sin perjuicio de informar que las medidas de seguridad en internet no son inexpugnables.

Teniendo en cuenta las disposiciones del Real Decreto 1720/2007, de 21 de diciembre, podemos establecer los siguientes derechos del usuario en lo que respecta a su privacidad:

- Derecho a oponerse a que su información personal sea utilizada en el caso de no haber obtenido anteriormente su consentimiento, cuando se quiera usar para fines publicitarios o de prospección comercial o cuando, del tratamiento de sus datos, se deriven decisiones que les afecten directamente.

- Autorización a los menores de más de 14 años a que sean ellos los que den el consentimiento para el tratamiento de sus datos personales.

- Derecho del usuario de preguntar en cualquier momento a la empresa suministradora del servicio, cuáles son los datos personales que maneja y con qué finalidad los está utilizando.

- Derecho del usuario para rectificar la información que no se encuentre actualizada, o para decidir cancelar el permiso que ha concedido para su utilización. Si una vez denegado el consentimiento por parte del usuario sobre el tratamiento de su información personal, la empresa continúa utilizando sus datos personales, podría incurrir en una sanción grave o muy grave, y ser sancionada con una multa que oscila entre los 60.000 y los 600.000€ en función de la sensibilidad de los datos que se utilicen.

Según este Real Decreto 1720/2007, de 21 de diciembre, el tratamiento de los datos ha de ser legítimo, debe adecuarse a la normativa establecida (Ley Orgánica de Protección de Datos, LOPD), es necesario informar a los usuarios sobre el mismo, y solicitar su consentimiento, debiendo quedar registrados los datos en un fichero que cumpla con la normativa establecida (Agencia Estatal de Protección de Datos, AEPD).

Dentro de la Unión Europea, podemos destacar la *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995*, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y la *Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 julio de 2002*, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (*Directiva sobre la privacidad y las comunicaciones electrónicas*).

Los objetivos principales de la *Directiva 95/46/CE de 24 de octubre de 1995* son, por un lado, proteger el derecho fundamental de protección de datos, y por otro, garantizar la libre circulación de los datos personales en la Unión Europea. Dice así: los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

Dentro de esta Directiva podemos destacar las siguientes disposiciones:

- Tratamiento de categorías especiales de datos (Artículo 8). Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

- Información en caso de obtención de datos recabados del propio interesado (Artículo 10).

- Información cuando los datos no han sido recabados del propio interesado (Artículo 11).

- Derecho de acceso (Artículo 12): Derecho de acceso del interesado a los datos.

- Confidencialidad y Seguridad del tratamiento de los datos (Artículos 16 y 17).

La Directiva 95/46/CE de 24 de octubre de 1995, ha sido derogada por el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016* para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por la Directiva que fija las normas sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos, y para las actividades judiciales correspondientes.

Dicho Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, destacando las siguientes disposiciones:

- Principios relativos al tratamiento de los datos personales, su licitud, consentimiento, tratamiento de categorías especiales de datos personales (Artículos 5, 6, 7, 9).
- Información y acceso a los datos personales (Artículos 13, 14).
- Derecho de acceso del interesado a los datos personales (Artículo 15).
- Derecho de rectificación y supresión (derecho al olvido), (Artículos 16, 17).
- Derecho a la limitación del tratamiento de los datos (Artículo 18).
- Derecho a la portabilidad de los datos (Artículo 20).
- Decisiones individuales automatizadas, incluida la elaboración de perfiles (Artículo 22).
- Protección de datos desde el diseño y por defecto (Artículo 25).
- Seguridad del tratamiento de los datos personales (Artículo 32).
- Evaluación de impacto relativa a la protección de datos (Artículo 35).
- Códigos de conducta y certificación (Artículos 40, 42).
- Transferencias de datos personales a terceros países u organizaciones internacionales (Artículos 44-50).

Por otra parte, la Directiva sobre la privacidad y las comunicaciones electrónicas, *Directiva 2002/58/CE de 12 de julio de 2002*, tiene como objetivo armonizar las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas de la Comunidad. En esta Directiva, destacamos las disposiciones relativas a:

- Seguridad de los servicios de comunicaciones electrónicas (Artículo 4).
- Confidencialidad de las comunicaciones (Artículo 5).
- Datos de tráfico (Artículo 6).
- Datos de la localización del usuario distintos de los datos de tráfico (Artículo 9).
- Características técnicas y normalización de los equipos terminales y otros equipos de comunicaciones electrónicas, que garanticen su compatibilidad con el derecho de los usuarios de proteger y controlar el uso de sus datos personales (Artículo 14).

Como vemos, la privacidad de nuestros datos se encuentra protegida de distintas formas tanto en nuestra legislación a nivel nacional, como a nivel europeo, por lo que debe considerarse como un hecho normal que la ley proteja los datos personales de cada individuo, sus comunicaciones, sus documentos privados, así como su propia imagen. Sin embargo, la gran cantidad de datos que son adquiridos y transferidos por todo el mundo, a través de las diferentes tecnologías utilizadas en las aplicaciones del AmI, hace que el derecho a la privacidad de la información de los usuarios se vea inmerso en un complejo marco legal, en el que convergen diferentes normas sobre los diferentes dispositivos de computación y comunicación.

4.3. IMPORTANCIA DE LA PRIVACIDAD EN AmI: MODELOS DE PRIVACIDAD.

Como ya se ha mencionado, la visión de la Inteligencia Ambiental consiste fundamentalmente en la creación de entornos inteligentes en los que los usuarios interaccionan de una forma natural, con diferentes servicios o aplicaciones a través de las tecnologías de la información y las comunicaciones (TICs). El objetivo en la construcción de estos sistemas es el de proporcionar soporte a los usuarios, facilitándoles la realización de las actividades cotidianas en los diferentes dominios en los que se encuentren: hogar, salud, educación, trabajo, ocio, etc.

La evolución y el uso de las tecnologías presentes en los dominios de aplicación de la Inteligencia Ambiental, inmersas en la mayoría de nuestras actividades diarias, nos ofrecen un mundo tecnológico cada vez más complejo que nos lleva a considerar el hecho de que, en general, los desarrollos tecnológicos avanzan más deprisa que su propia regulación a nivel legislativo.

En la actualidad, los rápidos cambios tecnológicos y la globalización han hecho surgir nuevos desafíos y oportunidades a nivel mundial, tanto para los gobiernos como para los ciudadanos en general, sobresaliendo el tema de la privacidad como uno de los valores sociales fundamentales que, cada vez más, está siendo objeto de mayor atención.

En el acceso de los usuarios a los servicios ofrecidos por el AmI, los diferentes dispositivos y tecnologías utilizados en los entornos inteligentes son capaces de adquirir, almacenar, gestionar y transmitir una gran cantidad de información y datos personales sobre los usuarios. Esta situación trae como consecuencia que los posibles usos que puedan realizarse sobre los mismos, haya elevado los riesgos relativos a la seguridad y protección de la privacidad de los usuarios.

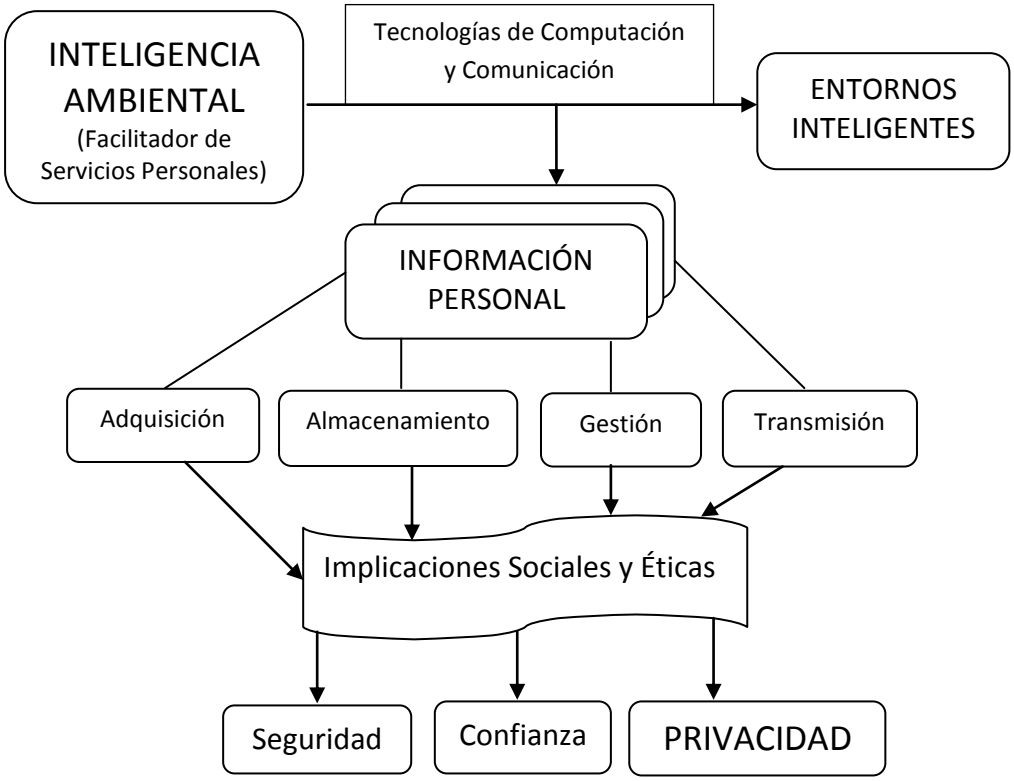

Figura 4.1. Implicaciones Sociales y Éticas del AmI

Como ya se ha mencionado, resultan evidentes las razones por las cuales las aplicaciones desarrolladas en los dominios de aplicación del AmI, en un mundo tecnológico cada vez más complejo, suponen un riesgo para la seguridad y privacidad de la información de los usuarios; esto es debido fundamentalmente a factores como:

- La facilidad para adquirir una gran cantidad de datos personales.
- La persistencia en el tiempo de dicha información.
- El almacenamiento y procesado de la información en una infraestructura remota, distribuida y dinámica.
- La integración de la información personal en varios sitios.
- La movilidad de la información en un entorno dinámico, en el que diferentes servicios y dispositivos pueden ser agregados e intercambiados, ofreciendo distintos tipos de servicios a los usuarios.
- El control y la transmisión de la información.
- La posibilidad de acceder y obtener información de una manera fácil.

Los sistemas desarrollados en AmI, están basados en contexto en el que podemos distinguir dos niveles: el nivel relativo a factores humanos y el nivel relativo al entorno físico *[H. Vagts, et al. 2011]*. La información de contexto relativa a los factores humanos puede ser clasificada en tres categorías: información relativa al usuario (conocimiento de sus hábitos, estado emocional, condiciones fisiológicas, etc.); información relativa al entorno social del usuario (su posición respecto a otras personas, interacción social, grupos, etc.); e información relacionada con las peticiones del usuario (actividades espontáneas, tareas que realiza, objetivos generales, etc.).

Por otro lado, la información relativa al entorno físico se puede clasificar en: información sobre la localización (posición absoluta, posición relativa, etc.); información sobre la infraestructura (diferentes dispositivos de computación, comunicación, ejecución de tareas, etc.); y la información relacionada con las condiciones físicas (ruido, luz, temperatura, etc.).

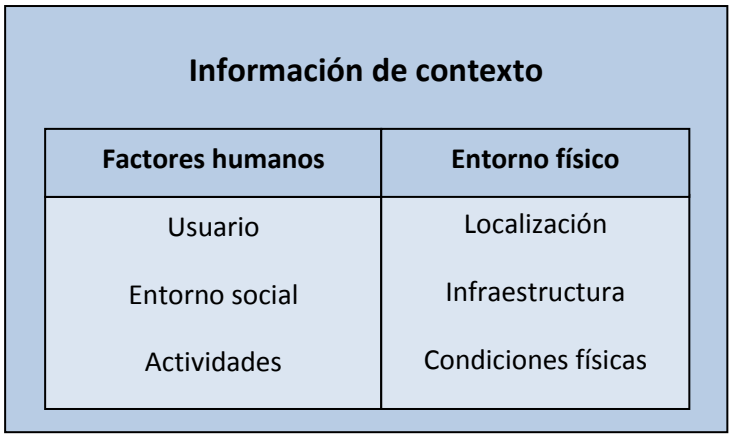

Figura 4.2. Tipos de Información contextual en AmI

Todas estas categorías de la información que definen el contexto del AmI deberán tenerse en cuenta a la hora de establecer las diferentes políticas de privacidad, que nos pueden ayudar a determinar el nivel de protección de los datos e información del usuario, según el dominio de aplicación en el que se encuentre.

En general, las prácticas legales y sociales evolucionan de acuerdo a las innovaciones de diseño y desarrollo tecnológicos, por lo que las buenas prácticas sobre los métodos de captura, distribución y uso de la información obtenida en los sistemas desarrollados en Inteligencia Ambiental, se determinarán con el paso del tiempo, teniendo en cuenta los diferentes tipos de uso de las aplicaciones del AmI (público o privado). Para que los servicios ofrecidos al usuario en los dominios de aplicación del AmI sean realmente beneficiosos, deben cumplirse las diferentes políticas de privacidad que se hayan establecido en cada situación, garantizándose así la confianza de los usuarios.

Como se ha indicado en el apartado anterior, la privacidad es uno de los derechos fundamentales de las personas que se encuentra protegido internacionalmente en tratados, directivas y en constituciones de diferentes países. La privacidad es un concepto complejo y personal que, dependiendo de la situación en la que se contextualice, puede ser interpretado de varias formas *[Bryce, C. et al. 2007]*. En *[Westin, A.F. 2003]*, se define la privacidad como el derecho de la persona para decidir qué información sobre ella puede ser conocida por otras personas y cómo pueden utilizarla.

La recopilación de información proveniente de distintas fuentes y su integración conjunta es denominada como "fusión de la información" por *[Sweeney. L. 2001]*, lo cual permite que la información privada pueda ser revelada. La gran cantidad de datos intercambiados entre los diferentes dispositivos presentes en las aplicaciones del AmI ofrece la posibilidad de realizar un filtrado de la información que puede identificar al usuario; este tipo de información se define como "privacidad de la información".

La adquisición de diferentes tipos de datos e información, y la disponibilidad de los mismos en los dominios de aplicación de la Inteligencia Ambiental, no son los únicos aspectos que deben tenerse en cuenta a la hora de evaluar los beneficios y desventajas de las aplicaciones del AmI, sino que también resulta necesario considerar el tipo de conocimiento que puede extraerse de los datos. Es evidente que los datos que ofrecen un mayor conocimiento sobre los usuarios son los denominados "perfiles de usuario" *[De Hert, P. et al. 2009]*. Puede ocurrir que el conocimiento sobre las personas extraído al acceder a los servicios ofrecidos por el AmI, origine irregularidades en la información entre los que están siendo observados (mediante la transmisión de su información) y los que están observando (accediendo a dicha información).

Los estudios sobre la privacidad en Inteligencia Ambiental se encuentran dirigidos principalmente en la obtención de conocimiento y control de la información recopilada y procesada. Sin embargo, muchas de estas aproximaciones dependen de políticas de privacidad que han sido especificadas previamente, o dan por hecho que los escenarios en los que tienen lugar son estáticos o limitados, por lo que no tienen en cuenta ni la adaptación dinámica de los sistemas, ni el desarrollo de estrategias de control sobre la privacidad, necesarias en la mayoría de las situaciones en las que se desarrollan las aplicaciones del AmI (entornos distribuidos y dinámicos); teniendo además en cuenta que el control de la privacidad es un proceso dinámico y selectivo *[Altman, I. 1975]*.

Algunos de los enfoques sobre la privacidad en Inteligencia Ambiental los encontramos en *[Langheinrich, M. 2002]*, *[Hong, J.I. et al. 2004a]*. Estos autores presentan mecanismos para mejorar el conocimiento de la privacidad y control de la información adquirida y procesada, aunque no ofrece ayuda a los usuarios en el proceso de configuración de la privacidad. Un estudio sobre la privacidad de la información relativa a la localización del usuario es el presentado en *[Krumm, J. 2009]*. Otros trabajos se encuentran focalizados en la privacidad sensible de la información de contexto *[Sheikh, K. et al. 2008]*, y en la manera en la que se intercambia la información para preservar la privacidad *[Hesselman, C. et al. 2008]*.

El proyecto de investigación presentado en *[Wright, D. et al. 2008]*, se encuentra dirigido hacia los aspectos sociales, económicos, legales, tecnológicos y éticos de la Inteligencia Ambiental, con especial interés en la privacidad, confianza, seguridad e identidad a través del estudio de cuatros escenarios "oscuros", que incluyen cuestiones individuales y sociales relacionadas con lo que se considera privado y lo que es público. El estudio realizado revela la existencia de riesgos, amenazas y vulnerabilidad, relacionados con la privacidad, confianza, seguridad, identidad e integridad, que se ve incrementada de manera notable en los escenarios en los que los dispositivos de vigilancia y monitorización presentes, pueden dar lugar a ataques maliciosos o dañinos.

En el trabajo presentado en *[Friedewald, M. et al. 2005]*, se incluyen más de setenta investigaciones y proyectos, teniendo en cuenta el tipo de escenarios, las suposiciones que deben hacerse sobre los usuarios, y el control sobre los sistemas desarrollados en AmI. El proyecto se extiende en cinco dominios de aplicación del AmI: hogar, salud, compras, trabajo, ocio y entretenimiento. El diseño y desarrollo de las aplicaciones del AmI requerirán un alto nivel de control sobre la seguridad, en aquellas situaciones en las que los sistemas no necesiten demasiada comunicación con los usuarios (por ejemplo, en las situaciones de catástrofes o emergencias); y tendrán un menor nivel de control cuando los sistemas desarrollen un papel de aconsejar o ayudar a los usuarios (en estos casos, el control sobre la seguridad puede estar subordinado al propio usuario).

El estudio llevado a cabo por *[Bohn, J. et al. 2004]* presenta las dos características fundamentales de la Inteligencia Ambiental, que son las que conforman los principales retos de privacidad a los que se enfrentan los sistemas desarrollados en AmI. Estas características son: por una parte, la habilidad de los sistemas del AmI para recoger una extensa y detallada cantidad de datos sobre los usuarios y sobre sus actividades cotidianas, durante largos periodos de tiempo; y por otra parte la creciente habilidad para integrar, buscar y recuperar esta información. Estos dos aspectos del AmI, resultan fundamentales para poder llevar a cabo uno de los principales objetivos del AmI que es el de ofrecer servicios personalizados. La Inteligencia Ambiental puede ofrecernos una ayuda compleja en nuestra vida cotidiana, pero las capacidades con las que puede utilizar la información obtenida, pueden ocasionar una extensa e invisible red rodeando al usuario (se puede decir que las paredes oyen). Los autores identifican además tres cuestiones adicionales que deben tenerse también en consideración en los entornos del AmI: la fiabilidad, la delegación del control, y la compatibilidad y aceptación social.

En *[Rouvroy, A. 2008]*, el autor considera las estrategias adoptadas en Europa sobre la protección de datos y la privacidad, con el objetivo de ver si resultan aplicables y adecuadas para las comunicaciones e intercambio de los diferentes tipos de datos que son recogidos y procesados en los entornos del AmI.

En el marco europeo sobre los derechos humanos se incorpora "la autonomía en la construcción de la identidad de cada individuo" de manera explícita, en lo que se refiere al derecho a la privacidad. Una consecuencia de esta declaración es el derecho de los individuos para controlar su información personal.

La ubicuidad de los sistemas desarrollados en AmI y su invisibilidad en la adquisición de la información, hacen que sea muy poco probable que el usuario tenga control acerca de los datos que están siendo recopilados y registrados ya que, en muchos casos, ni siquiera es consciente de la existencia de estos sistemas. Además, teniendo en cuenta que otro de los objetivos de los sistemas desarrollados en AmI es el de conocer los perfiles de los usuarios con el fin de responder a sus necesidades, se plantea la cuestión de que estas necesidades pueden haber sido establecidas por los propios sistemas y, por consiguiente, por los diseñadores de los mismos, y no por el usuario; lo que pone en cuestión el derecho de control de los usuarios. En estos dos últimos estudios [Bohn, J. et al. 2004] y [Rouvroy, A. 2008], se comparte la preocupación sobre la delegación del control de la información en los sistemas distribuidos del AmI, en los que múltiples agentes artificiales y humanos, han de colaborar e interactuar, controlando los datos e información de los usuarios.

Varias de las investigaciones revisadas intentan cuantificar la privacidad utilizando diferentes tipos de medidas. En *[Reiter, M. et al. 1999]*, los autores emplean como medida de la privacidad el tamaño del set del anonimato (todos los sujetos potenciales que tienen la posibilidad de enviar/recibir información) para medir el grado de anonimato. Con este enfoque, los autores asumen que cada remitente del set, presenta la misma probabilidad en el envío de un mensaje.

El estudio presentado por *[Serjantove, A. et al. 2002]* utiliza la entropía para medir el grado de anonimato que puede conseguir un sistema. Otro estudio que utiliza la entropía como medida de los niveles de privacidad es el presentado en *[Díaz, C. et al. 2002]*. Una entropía diferencial es la medida utilizada por *[Agrawal, D. et al. 2001]* para cuantificar la cercanía del valor de un atributo con un valor en conflicto con su valor original.

En el estudio presentado en *[Hong, J.I. et al. 2004b]*, los autores proponen un modelo que basado en el control y el feedback. En este trabajo, los autores sugieren que los diseñadores del AmI deberían realizar un análisis de los riesgos de privacidad, teniendo en cuenta el contenido de tipo organizativo y social. Este tipo de análisis debe tener en cuenta cuestiones como: ¿Quiénes son los usuarios?, ¿Qué tipo de información es la que está siendo compartida?, ¿Cómo es la información personal recogida? Los autores consideran que, después de realizar el análisis inicial de los riesgos de privacidad, los diseñadores necesitan priorizar los resultados y gestionar los registros de estos riesgos de privacidad.

El modelo de gestión de la privacidad propuesto en *[Friedewald, M. et al. 2007]* incluye varios componentes entre los que se encuentran: los participantes, el entorno, la actividad, la transmisión de la información, los niveles de control así como la tecnología disponible. La visión de la privacidad considerando sus preferencias y limitaciones, y el uso del lenguaje computacional para representarlas, se presentan en el estudio de *[Adams, A. et al. 2001]*. En el trabajo de *[Kapadia, A. et al. 2007]* se utilizan paredes virtuales para gestionar la privacidad. En [Lederer, S. et al. 2002], el modelo propuesto por los autores considera un nivel de privacidad preferencial que depende de la legislación, las características de mercado, los estándares, las tecnologías utilizadas, la naturaleza de la información divulgada, las características del contexto, la información sensible, las características de la información del usuario, y la previsión de lo que supone el coste del modelo frente a los beneficios.

Otros autores consideran los modelos de recomendación y confianza como una de las estrategias más útiles en los sistemas ubicuos, que pueden servirnos para proteger nuestra privacidad, como queda reflejado en los trabajos presentados por *[Garimella Rama Murthy, 2006]*, *[Abdul-Rahman, A. et al. 2000]*, *[Billhardt H. et al. 2007]*, *[McKnight DH, et al. 2002]*, *[Liu Z, Yau et al. 2008]*, *[Lu Y. et al. 2006]*, *[Almenarez F, et al. 2004]*.

La divulgación de los datos significa la pérdida de la privacidad por lo que, si se tiene un nivel alto de confianza en la manera en la que se transmiten éstos, podemos reducir los riesgos de la misma [Ruotsalainen, PS. et al. 2012].

4.4. CONCLUSIONES

El gran desarrollo de las aplicaciones del AmI que se ha producido en la última década ha llevado a muchos investigadores a plantearse diversas cuestiones relacionadas con el diseño y desarrollo de modelos de privacidad, servicios, y arquitecturas que ofrezcan unos niveles de privacidad aceptables para los usuarios. Muchos de estos modelos de privacidad desarrollados han resultado de utilidad en los entornos ubicuos del AmI.

Las investigaciones sobre los modelos de privacidad en AmI se encuentran principalmente orientadas a la obtención del conocimiento y control de la información que se recopila y procesa. Gran parte de estos enfoques dependen de políticas de privacidad preestablecidas o asumen que los escenarios en los que se desarrollan los servicios ofrecidos por el AmI se encuentran restringidos.

La mayoría de los estudios realizados sobre las aplicaciones desarrolladas en Inteligencia Ambiental, se encuentran focalizados en el uso y mejora de los dispositivos tecnológicos (encargados de la computación y comunicación de la información); en algunos casos se centran en los usuarios (accesibilidad); y en muy pocos casos van dirigidos al tratamiento de cuestiones de tipo social y ético que suponen el uso de estas tecnologías; aunque resulta ampliamente aceptado el gran impacto que tienen la seguridad y privacidad de la información de los usuarios al acceder a los servicios personalizados ofrecidos por el AmI, tal y como queda reflejado en los diferentes trabajos mencionados. Para abordar los riesgos que afectan a la privacidad, no solo es necesario presentar soluciones de tipo técnico relacionadas con: encriptación y autenticación, diferentes protocolos de privacidad y seguridad, sistemas para el control del acceso a las aplicaciones, separación de los recursos disponibles, etc., sino que resulta fundamental tener en cuenta las diferentes las políticas de privacidad que deben ser conformes a la situación en la que nos encontremos.

La privacidad se ha convertido en un valor fundamental para los usuarios, a la hora de valorar la calidad de los servicios ofrecidos por las aplicaciones del AmI. Una de las principales preocupaciones de los usuarios sobre la obtención y almacenamiento de su información personal, consiste en saber quién puede acceder y/o modificar el contenido de la misma. Por otra parte, el desconocimiento por parte de los usuarios de la existencia de dispositivos de computación y comunicación, que pueden acceder a su información personal y divulgarla, al utilizar un determinado servicio, es otro de los aspectos que suscita intranquilidad en los usuarios. Los usuarios han de conocer la existencia de estos sistemas y deben poder saber cómo utilizan la información que obtienen. Con el fin de garantizar la privacidad de los usuarios, es necesario que los sistemas desarrollados en Inteligencia Ambiental tengan en cuenta las diferentes políticas de privacidad establecidas en cada situación, ofreciendo a los usuarios herramientas que les faciliten estas tareas y les ayuden a minimizar los riesgos de la privacidad de su información personal.

En nuestras relaciones sociales, solemos compartir nuestra intimidad con las personas que nos inspiran un mayor grado de confianza. La privacidad y la confianza son conceptos que se encuentran muy interrelacionados entre sí, por lo que resulta adecuado considerarlas juntas para abordar los aspectos socio-éticos presentes en las aplicaciones del AmI.

Confiar en los servicios ofrecidos por las tecnologías utilizadas en las aplicaciones desarrolladas en Inteligencia Ambiental, nos puede ayudar a minimizar los riesgos relacionados con nuestra privacidad.

PARTE III

PROPUESTA, DESARROLLO Y CASO DE ESTUDIO

Capítulo 5

Marco Conceptual de Privacidad en AmI

5.1. PRIVACIDAD EN EL DISEÑO DEL AmI

La mayoría de los estudios realizados sobre las aplicaciones desarrolladas en Inteligencia Ambiental se encuentran dirigidos hacia cuestiones relacionadas con las tecnologías involucradas (dispositivos de computación y comunicación), y en algunos casos se centran en el usuario. Teniendo en cuenta que, uno de los principales objetivos en el desarrollo de las aplicaciones de la Inteligencia Ambiental es el de ofrecer servicios personalizados, consideramos que el elemento principal que debe tenerse en cuenta en el desarrollo de las mismas es el usuario. Debe ser la aplicación la que se adapte a las características y requerimientos del perfil de los usuarios al acceder a un determinado servicio, destacando la privacidad como una de las principales cuestiones que deben ser consideradas en el diseño de las mismas.

A continuación se presenta un ejemplo de una aplicación general desarrollada en AmI, que pone en evidencia los riesgos de privacidad de la información personal de los usuarios en el acceso a un determinado servicio, mediante una aplicación web. En el acceso a la aplicación, los usuarios proporcionan sus datos o información de carácter personal, quedando ésta registrada en ficheros que son propiedad del titular de la empresa proveedora de ese servicio (en cumplimiento con la L.O. 15/1999 Protección de Datos de Carácter Personal y su normativa de desarrollo).

Estos datos personales pueden ser utilizados con dos finalidades: (A) La empresa puede gestionar los datos en el propio sistema web, o en la aplicación desarrollada. (B) La empresa puede utilizarlos para el envío de comunicaciones sobre diferentes actividades como puede ser el envío de productos ofertados, o el envío de otros servicios. En este punto, es importante destacar que debe existir una aceptación por parte del usuario, autorizando a dicha empresa, la utilización o tratamiento de sus datos personales (responsabilidad del usuario) para las finalidades que hayan sido acordadas, y que deben estar claramente definidas. Por último el registro de los ficheros de datos, debe ser notificado ante el Registro General de la Agencia Española de Protección de Datos (AEPD).

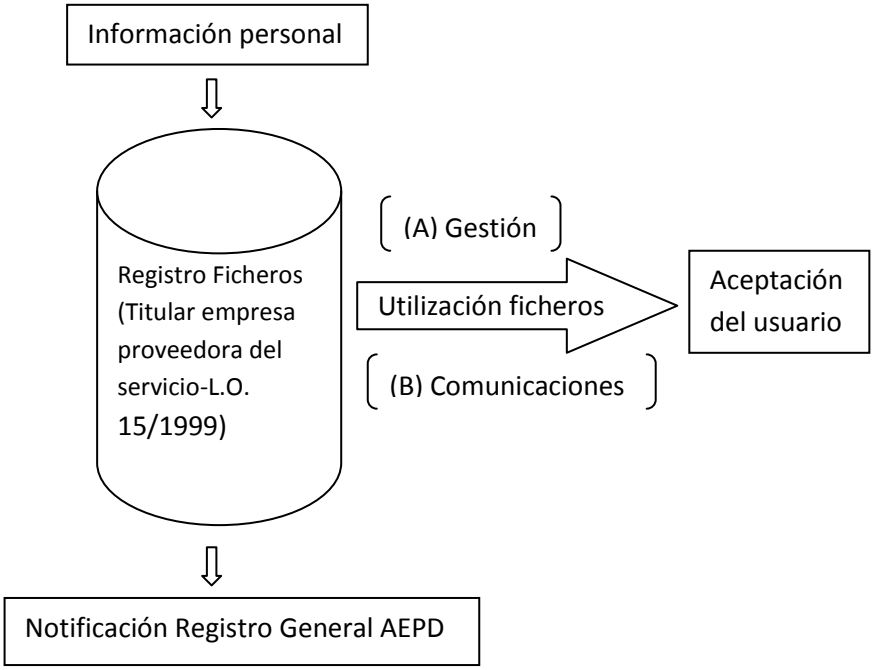

Figura 5.1. Ejemplo de acceso a un determinado servicio web desarrollado en AmI

Analizando las secuencias descritas, nos encontramos con las siguientes cuestiones que representan una amenaza para la protección de privacidad de la información de los usuarios:

- El titular de la empresa proveedora del servicio al que acceden los usuarios, es el responsable del fichero donde quedan almacenados y registrados los datos o información personal de los usuarios. Sin embargo, dicha empresa no se responsabiliza de que esta información pueda obtenerse a través de distintas aplicaciones móviles, que puedan ser incluidas; es más, indica que estas aplicaciones móviles deberán tener sus propios responsables, así como sus propias condiciones legales y términos de uso (hecho totalmente desconocido por los usuarios).

- La empresa proveedora del servicio ofrecido al usuario es también responsable de la gestión de toda la información personal almacenada. Cada servicio prestado por la empresa proveedora debe estar sujeto a su legislación nacional correspondiente. En este punto, cabe destacar que el usuario debería conocer y autorizar el uso y tratamiento que la empresa hace con sus datos personales (finalidad A). Además, el usuario debe disponer de una manera fácil y gratuita la forma de oponerse a recibir información o comunicaciones de la empresa proveedora del servicio (finalidad B), por ejemplo mediante un correo electrónico donde pueda notificar su oposición o aceptación. El usuario tiene el derecho de poder conocer y solicitar en cualquier momento a la empresa suministradora del servicio o producto solicitado, cuáles son los datos personales que maneja y con qué finalidad los utiliza, pudiendo en cualquier momento rectificarlos, y/o cancelar el permiso que haya concedido inicialmente para su utilización.

Con este sencillo ejemplo, vemos que resulta fundamental tener en consideración las cuestiones relativas a la privacidad de nuestra información personal, en el diseño de las aplicaciones desarrolladas en Inteligencia Ambiental. Los principales aspectos que deben tenerse en cuenta en el diseño de la privacidad "Privacy by Design" de las aplicaciones del AmI, basadas en el dominio de aplicación y centradas en el usuario son *[Clarke, R. 1997]*:

- *Privacidad de los datos* (privacidad de la información). Los usuarios reclaman que la obtención de datos o información acerca de ellos, no debería estar disponible para otros usuarios u organizaciones; y que en el caso de que esta información haya sido adquirida por terceras partes, el usuario ha de tener la capacidad de ejercer un grado de control significativo sobre la misma, y sobre su utilización.

- *Privacidad del comportamiento personal* (privacidad mediática). Este aspecto se refiere a las cuestiones relacionadas con el comportamiento o forma de ser de los usuarios, especialmente la información referida a asuntos sensibles o confidenciales (delicados/íntimos), como pueden ser las preferencias o hábitos sexuales, las relacionadas con las ideas políticas y prácticas religiosas, ya sea en el ámbito privado como en el ámbito público.

- *Privacidad de la experiencia personal*. La gran cantidad de información que puede ser recogida a través de las diferentes experiencias que vivimos a diario, ofrece la capacidad de poder ser utilizada (y de hecho se utiliza), llevándose a cabo en muchos de los casos de forma maliciosa. Algunas de las acciones que llevan a cabo los usuarios, y que son fuente de adquisición de este tipo de información, son las referidas a la adquisición de libros, periódicos, imágenes, vídeos, conversaciones con otras personas (tanto cara a cara como a través del teléfono móvil), reuniones con otros grupos de personas.

El entorno de las aplicaciones del AmI es distribuido y dinámico, diferentes servicios y dispositivos de computación y comunicación pueden ser agregados e intercambiados, para ofrecer distintos tipos de servicios a los usuarios. Además, en la mayoría de las aplicaciones desarrolladas en AmI observamos que los datos e información personal de los usuarios son almacenados y procesados en una infraestructura remota, distribuida y dinámica. Estas cuestiones hacen que la información personal de los usuarios, pueda moverse dentro de una misma organización, o a través de varias, sin su conocimiento en la mayoría de los casos, e incluso sin su consentimiento, por lo que se requiere una adecuada protección de la privacidad de dicha información, a través de diferentes tipos de acuerdos legales entre los diversos servicios ofrecidos al usuario y los dispositivos involucrados.

Todas estas reflexiones son las que nos llevan a considerar el término de privacidad en el diseño de las aplicaciones del AmI, “Privacy by Design”, cuyo principal reto es el de tener en cuenta las diferentes políticas de privacidad que se establezcan en cada situación, y la manera de fusionarlas en un determinado dominio del AmI.

En los dominios de aplicación del AmI estudiados hemos destacado la siguiente información del usuario que puede ser susceptible de verse amenazada:

- La información relacionada con sus datos personales.
- La información derivada de su comportamiento o forma de ser (información sensible/confidencial).
- La información obtenida a través de sus actividades o experiencias al interaccionar con los sistemas del AmI.

Por ello, en el diseño de las aplicaciones del AmI, se necesita llevar a cabo la identificación de los diferentes niveles de privacidad, establecidos según el dominio de aplicación del AmI en el que se encuentre el usuario. De esta forma, se podrán desarrollar los mecanismos más adecuados para establecer las consideraciones que puedan suponer una amenaza en la protección de nuestra información personal, y actuar en consecuencia.

Teniendo en cuenta estas consideraciones se presenta el marco conceptual de privacidad en AmI, que deberá garantizar el cumplimiento de las diferentes políticas de privacidad establecidas según el dominio de aplicación del AmI, y que servirá para determinar el nivel de protección requerido de la información; diseñando así la aplicación de forma que minimice los riesgos relativos a la privacidad de los usuarios.

5.2. MARCO CONCEPTUAL DE PRIVACIDAD EN AmI

Para el diseño del marco conceptual de privacidad en AmI, se han establecido diferentes políticas de privacidad, teniendo en cuenta los dominios de aplicación de la Inteligencia Ambiental, y teniendo como principal objetivo al usuario. El marco conceptual propuesto, consta del Sistema de gestión de la privacidad, y del Agente controlador de privacidad de los datos. Estos dos sistemas tienen en consideración las interacciones entre las diferentes tecnologías y dispositivos utilizados, con los usuarios dependiendo del dominio de aplicación en el que se encuentren.

Este marco conceptual de gestión de la privacidad, puede ayudarnos a poner en práctica el concepto "Privacy by Design", en el cual, las tecnologías y procesos utilizados para proteger la privacidad son tenidos en cuenta a priori en el diseño de la propia arquitectura del sistema desarrollado, y no son añadidos a posteriori. De esta forma, podemos establecer las políticas de privacidad que deben cumplir tanto el Sistema de gestión de la privacidad, como el Agente controlador de privacidad de los datos, con el fin de minimizar los riesgos de privacidad de la información en un determinado dominio de aplicación del AmI.

Es importante destacar que, las diferentes políticas de privacidad establecidas en el diseño del marco conceptual de privacidad en AmI, deberán preservar ésta en diferentes niveles:

- Nivel de acceso a los datos. El acceso a la información relativa a los datos personales debe estar controlado, ha de ser visible, y estar disponible solamente para los administradores del sistema autorizados. Esto implica que el acceso de los usuarios debe ser restringido.

- Nivel de regulación de responsabilidades. Delegar responsabilidades sobre la integridad de la privacidad de los datos. Ésta puede estar en los usuarios, o en los proveedores de los servicios ofrecidos en la aplicación.

- Nivel de localización de los datos. Resulta necesario conocer dónde se encuentra alojada la información de los usuarios.

- Nivel de distribución de los datos. La mayoría de los datos pueden ser compartidos en otros dominios, o ser compartidos por otros proveedores de servicios de la aplicación, por lo que el usuario debe saber que las técnicas de encriptación utilizadas son seguras y efectivas.

- Nivel de recuperación de los datos. En el caso de que se produzca un fallo en el sistema, el usuario ha de saber lo que ha ocurrido, y lo que puede pasar con su información almacenada.

- Nivel de soporte técnico para investigar actividades ilegales. El registro de los datos puede estar localizado en otro centro de datos o cambiar de servidor, por lo que resulta necesario disponer de un agente que dé soporte específico para controlar o investigar cualquier tipo de actividad ilegal que pueda producirse en el registro de los datos personales del usuario.

Teniendo en cuenta estos niveles de privacidad, se presenta a continuación el marco conceptual de privacidad en AmI propuesto, en el que se distinguen los dos módulos que lo conforman, el Sistema de gestión de la privacidad (Privacy Management System), y el Agente controlador de privacidad de los datos (Privacy Data Controller Agent). Las diferentes políticas de privacidad consideradas en el diseño del modelo, se basan en las interacciones de las tecnologías y dispositivos utilizados con el usuario, según sea el dominio de aplicación del AmI en el que tienen lugar.

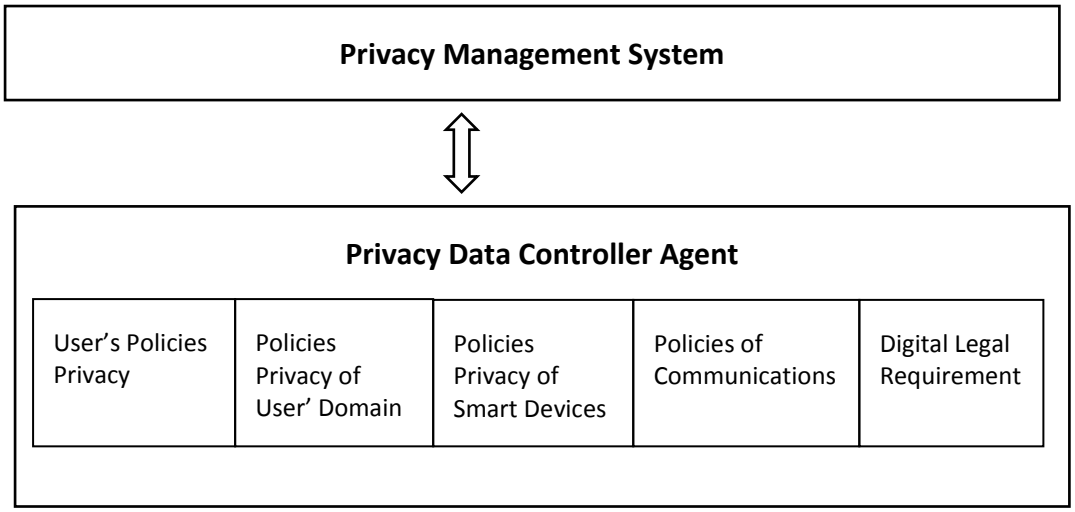

Figura 5.2. Modelo conceptual "Design by Privacy" en Inteligencia Ambiental

El Sistema de gestión de la privacidad ha de incluir mecanismos que aseguren que los agentes implicados en el controlador de la privacidad de los datos, disponen de medidas de protección adecuadas al procesar y transmitir la información personal, así como medidas para responder ante cualquier tipo de incidente o amenaza. Entre las medidas de protección que debe incluir el Sistema de gestión de la privacidad destacamos las siguientes:

- Disposiciones dirigidas al cumplimiento o conformidad de las políticas de privacidad establecidas en el Agente controlador de privacidad de los datos.
- Protocolos que notifiquen cualquier tipo de fallo de seguridad en el Agente controlador de privacidad.
- Disposiciones o planes para responder ante cualquier incidente o consulta.
- Disposiciones dirigidas a la realización de procesos de auditorías.
- Actualizaciones y revisiones continuas que aseguren, que el Agente controlador se encuentra en consonancia con un posible riesgo real en un determinado contexto.

Estas consideraciones hacen que el Sistema de gestión de la privacidad tenga que ser flexible y presente la capacidad de adaptarse al número y grado de sensibilidad de los diferentes procesos llevados a cabo por el Agente controlador de privacidad de los datos, que deberá tener en cuenta las medidas de protección indicadas. Asimismo, el Sistema de gestión de la privacidad deberá desarrollar las protecciones adecuadas, teniendo en cuenta la evaluación de los riesgos de la privacidad, que incluye diferentes procesos de identificación, análisis y evaluación de los riesgos de privacidad de la información, considerando el contexto en el que ha sido adquirida y/o gestionada dicha información.

El Agente controlador de privacidad de los datos (Privacy Data Controller Agent), consta de cinco módulos diferentes:

- El primer módulo tiene en cuenta, las políticas de privacidad propias del usuario al acceder a un determinado servicio o aplicación (User´s Policies Privacy).
- El segundo módulo corresponde a las políticas de privacidad específicas que definen el dominio de aplicación en el que se encuentra el usuario (Policies Privacy of User´s Domain).
- El tercer módulo incluye las políticas de privacidad propias de los dispositivos utilizados en la aplicación (Policies Privacy of Smart Devices).
- El cuarto módulo (Policies of Communications), engloba políticas de privacidad que afectan a las comunicaciones entre el usuario y el proveedor del servicio, o la aplicación utilizada.
- Y por último, el quinto módulo engloba diferentes requerimientos legales (Digital Legal Requirement), que pueden ser a nivel particular, obligaciones nacionales, obligaciones internacionales, programas auto-reguladores, disposiciones contractuales, etc.

Todos estos módulos, deberán incluir diferentes aspectos sobre las políticas de privacidad, relacionados con cuestiones como:

- Generalidades y características de la aplicación teniendo en cuenta el dominio en el que se encuentre el usuario.
- Definición de los objetivos de privacidad que hayan sido establecidos.
- Identificación de las amenazas que afectan a estos objetivos.
- Controles técnicos de protección frente a estas amenazas.
- Valoración de los riesgos de privacidad.

El modelo conceptual de privacidad en AmI, nos ayudará a determinar las políticas de privacidad de las aplicaciones, teniendo en cuenta el dominio en el que se desarrollan. Estas políticas de privacidad deberán incluir los diferentes niveles de protección de la información descritos anteriormente (Acceso a los datos, Regulación de Responsabilidades; Localización, Distribución y Recuperación de los datos, y Soporte técnico para actividades ilegales), sobre el modo en el que en un determinado dominio de aplicación del AmI, se adquiere, almacena, gestiona, comparte y transmite, diferentes tipos de información personal.

A partir del modelo conceptual de privacidad en AmI presentado, y atendiendo a las características que presentan tanto el Sistema de gestión, como el Agente controlador de privacidad de los datos, se han establecido las diferentes políticas de privacidad que deben ser consideradas en el diseño de las aplicaciones del AmI, atendiendo al dominio en el que se desarrollan. Estas políticas de privacidad, nos permiten determinar el nivel o grado de protección requerido de la información personal de los usuarios, según el dominio de aplicación del AmI en el que se encuentre. En la siguiente figura, se muestran los niveles de protección de la información que han sido determinados atendiendo a diferentes consideraciones: de tipo general, las relativas al usuario, las relacionadas con las características de los dispositivos y, las relacionadas con las comunicaciones. Se ha considerado que las relativas a las condiciones del usuario, son las que tienen un mayor peso en la determinación del nivel de protección de la información.

Dominio de Aplicación del AmI	Consideraciones Generales	Condiciones Usuario	Características Dispositivos	Características Comunicaciones	Nivel Protección Información
Salud/Smart House/Tecnologías de Asistencia (AAL)	El cuidado de la salud determina las condiciones de vida de las personas. El acceso a la información sobre el estado de salud de los usuarios puede resultar vital en caso de emergencia.	Pacientes o usuarios independientes, o con algún grado de dependencia. Pacientes o usuarios con algún tipo de capacidad mental limitada de forma permanente o transitoria (Ejemplo: problemas de corazón, derrame cerebral, epilepsia, etc.).	El carácter visible o invisible de los dispositivos no es muy importante, ya que hay consentimiento por parte del paciente o usuario en el uso del dispositivo.	El sistema necesita ser capaz de identificar al usuario. La transmisión de la información significa concesión por parte del usuario para preservar la: confidencialidad, integridad, disponibilidad de la información personal.	ALTO
Educación	En este dominio de aplicación, el interés general del público consiste en la protección de sus datos personales.	Las personas muestran interés por aprender en diferentes etapas de su vida, desde cualquier lugar, público o privado, y en cualquier momento.	El carácter visible o invisible de los dispositivos no es muy importante, ya que hay un acuerdo entre el usuario y la entidad educativa que permite el uso del dispositivo.	El sistema necesita ser capaz de identificar al usuario. La transmisión de la información significa concesión por parte del usuario para preservar la: confidencialidad, integridad, disponibilidad de la información personal.	MEDIO
Comercio y Negocio/Servicios Públicos y Transporte	En este dominio, el interés general del público consiste en la protección de sus datos personales.	Usuarios de los servicios públicos y transportes, negocios, ventas.	El usuario debe estar de acuerdo con el uso de los servicios de geo-localización, que se encuentran disponibles en los dispositivos utilizados.	El sistema necesita ser capaz de identificar el dispositivo utilizado (no resulta necesaria la identificación del usuario). La transmisión de la información significa concesión por parte del usuario para preservar la: integridad y disponibilidad de la información personal.	BAJO
Ocio y Entretenimiento	El interés general de los usuarios se encuentra en proteger sus datos personales (Ejemplo: adquisición, almacenamiento de información personal sin conocimiento de los usuarios).	Consumidores	En este tipo de dominio de aplicación, los dispositivos podrían no estar visibles para el usuario (Ejemplo: chip RFID).	El sistema necesita ser capaz de identificar al usuario. La transmisión de la información significa concesión por parte del usuario para preservar la: integridad y disponibilidad de la información personal	MEDIO

Tabla 5.1. Políticas de privacidad en los Dominios de Aplicación del AmI

5.3. CONCLUSIONES

El marco conceptual de privacidad en AmI propuesto, debe ser considerado como un paso hacia el establecimiento de guías o directrices de privacidad en el diseño de las aplicaciones de la Inteligencia Ambiental, “Design by Privacy” con la intención de que los usuarios al acceder a un determinado servicio o aplicación desarrollado en AmI, sean capaces de saber y entender lo que el sistema está haciendo con su información personal, y para qué puede ser utilizada.

Las políticas de privacidad establecidas por el Agente controlador de privacidad de los datos, pueden ayudarnos a minimizar los riesgos de privacidad de nuestra información personal, al acceder a las aplicaciones desarrolladas en Inteligencia Ambiental.

En la actualidad, la privacidad se ha convertido ya en un valor de calidad para los usuarios. Por ello, las tecnologías y dispositivos utilizados en los entornos inteligentes creados en Inteligencia Ambiental, deben ayudarnos a saber cómo y para qué se utilizan nuestros datos e información personal, cuando nos encontramos en un determinado dominio de aplicación del AmI.

Para que los sistemas desarrollados en AmI sean de calidad, y ofrezcan servicios personalizados a los usuarios deben considerarse no solo las cuestiones de tipo técnico, sino que deben tenerse en cuenta otros factores que juegan un papel fundamental en los dominios de aplicación del AmI, como son la accesibilidad, la normativa legal, y sobre todo las cuestiones de tipo ético, entre las que destaca la privacidad. La calidad en el grado de protección de la privacidad, depende en gran medida de las políticas de privacidad que se hayan establecido en el diseño de las aplicaciones desarrolladas en Inteligencia Ambiental.

Capítulo 6

Modelo de Privacidad Digital en AmI basado en Sistemas Multiagente

6.1. CONSIDERACIONES GENERALES

Una vez establecidas las políticas de privacidad, que nos han permitido evaluar el nivel de protección requerido de la información personal de los usuarios, según el dominio de aplicación del AmI, se presenta a continuación el Modelo de Privacidad Digital en Inteligencia Ambiental basado en Sistemas Multiagente.

Como se ha descrito en el capítulo 3 (Apartado 3.5.4.), las capacidades y características de los Agentes Inteligentes y de los Sistemas Multiagente, resultan una herramienta idónea para llevar a cabo la gestión y control de nuestra información personal, ya que pueden actuar como mediadores en las comunicaciones entre los agentes implicados en el sistema, intercambiando diferentes tipos de mensajes sobre la información adquirida, almacenada o compartida, teniendo en cuenta las políticas de privacidad establecidas.

Este modelo nos ayudará a minimizar los riesgos de privacidad de nuestra información en un dominio específico del AmI, se ha elegido para ello el entorno de experimentación sobre la confianza y reputación con agentes ART testbed (Agent Reputation and Trust) *[K. Fullam, et al. 2005]*, en el que los agentes, que han de confiar unos en otros, tienen el rol de tasadores de cuadros. Estos agentes hacen uso de un modelo de confianza interno con el que tomarán la decisión de elegir con quién comparten sus opiniones privadas, y con quién no, atendiendo a la reputación de los agentes implicados en la interacción. Este entorno fue definido mediante el esfuerzo conjunto de investigadores de múltiples países, y con él se han realizado diversas competiciones internacionales de agentes en el marco de la conferencia AAMAS (Autonomous Agents and Multiagent Systems) que han servido para validar los modelos de confianza y reputación.

Nuestro Modelo de Privacidad Digital en AmI basado en Sistemas Multiagente, tiene en consideración las políticas de privacidad establecidas en la configuración del Agente controlador de privacidad (Modelo conceptual "Privacy by Design"), las cuales nos han servido para establecer las decisiones que deben tomar los agentes involucrados en el sistema, para proteger la privacidad de la información transmitida en sus comunicaciones.

El Modelo de Privacidad Digital en AmI basado en Sistemas Multiagente presentado, mediante su implementación integrada en un modelo de confianza del entorno de experimentación ART, nos ayudará a decidir con qué agentes compartimos nuestras opiniones privadas, y con cuáles no, teniendo en cuenta si son de confiar o no, minimizando así los riesgos de privacidad de nuestra información personal. Es decir, compartiremos nuestras opiniones privadas con aquellos agentes en los que confiemos.

6.2. MODELOS DE CONFIANZA Y PRIVACIDAD

La confianza es una de las cuestiones que más valoramos en nuestras relaciones sociales, junto con la privacidad, incluso cuando estas relaciones tienen lugar a distancia, e incluso cuando presentan un sentido electrónico. Decimos que una persona nos inspira confianza cuando tenemos trato íntimo o familiar con ella, es decir cuando compartimos con esa persona nuestros asuntos y opiniones más personales. En nuestras relaciones sociales, lo habitual es que compartamos nuestros asuntos más personales con aquellas personas que nos ofrecen confianza, lo cual quiere decir que no van a divulgar ni modificar dicha información.

Estas consideraciones, han llevado a numerosos investigadores a interesarse por el estudio de cómo se adquiere y se mantiene la confianza; en especial cuando los usuarios son representados por agentes autónomos que actúan de manera electrónica en nombre de ellos, teniendo en cuenta los intereses de los usuarios, a la hora de tomar decisiones y relacionarse entre ellos.

Esta es la idea que representan los modelos de confianza, en los cuales la cooperación es una consecuencia de la confianza.

Un modelo de confianza puede ser aplicado mediante agentes inteligentes de dos maneras: la primera de ellas es buscando socios en los que confiar, y la segunda consiste en utilizarlo como mecanismo social de tipo premio/castigo, con el fin de prevenir cualquier tipo de actuación o comportamiento incierto, voluble o deshonesto por parte de algún agente. En los modelos de confianza, cada tipo de acción que lleva a cabo un agente autónomo puede ser evaluada, lo cual nos permite poder evaluar la reputación de la imagen que ofrece cada agente (entendiendo por reputación la opinión o estimación del agente, su prestigio o fama).

Existen varias formas de evaluar la reputación de un agente. Una de ellas consiste en evaluar su reputación de una manera centralizada (como una propiedad general representada por una entidad única), así es como tiene lugar en la mayoría de las aplicaciones comerciales *[C. Dellarocas, 2003]*; pero esto conlleva pérdidas en la personalización y también en la privacidad. Por ello, consideramos (en consonancia con la mayoría de los investigadores en Inteligencia Artificial Distribuida), que cada miembro de la sociedad de agentes tiene que encargarse de evaluar la reputación de todos los demás agentes que forman parte de esa sociedad, o al menos la de aquellos con los que interactúa de forma directa o indirecta.

Se han propuesto muchos modelos de confianza con diferentes características *[J. Sabater-Mir, C. Sierra, 2005]*; pero en la mayoría de ellos se consideran como las principales fuentes de información, por un lado las experiencias directas, y por otro lado la información declarada. Entre estas dos fuentes de información, hemos considerado como fuente de información principal de nuestro modelo, la información declarada; ya que consideramos que este tipo de información tiene mayor relevancia en lo que respecta a la privacidad.

La información declarada (*witness information*) es también conocida como información indirecta, o como información "de boca a boca". Es la información que un agente (llamado en adelante 1st Agent, First Agent) recibe de otro agente (2nd Agent, Second Agent), acerca de un tercer agente (3rd Agent, Third Agent). Este tipo de información puede estar basada en las experiencias del segundo agente, o puede basarse en la información indirecta de otros agentes, llamados Agentes de Referencia (Referral Agents).

En gran parte de los modelos de confianza, el 2nd Agent solo comparte la imagen de reputación del 3rd Agent (uniendo sus experiencias directas y la información declarada); este es el método clásico de compartir la reputación. Las cuestiones sobre privacidad de cómo este 3rd Agent se comporta con el 2nd Agent, se encuentran incluidas en este modelo clásico de información declarada (*classic witness information*).

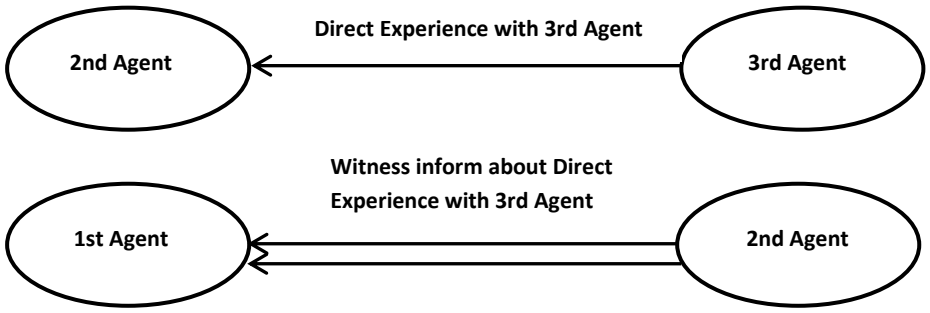

Figura 6.1. Esquema de cómo se lleva a cabo la comunicación en el método clásico

En otros modelos de confianza se incluye la información declarada del 3rd Agent y también de los Agentes de Referencia (Referral Agents), formándose así una cadena de confianza *[B. Yu, M.P. Singh, 2002]*, *[B- Esfandiari, S-Chandrasekharan, 2001]*, que hace aumentar los problemas relacionados con la privacidad.

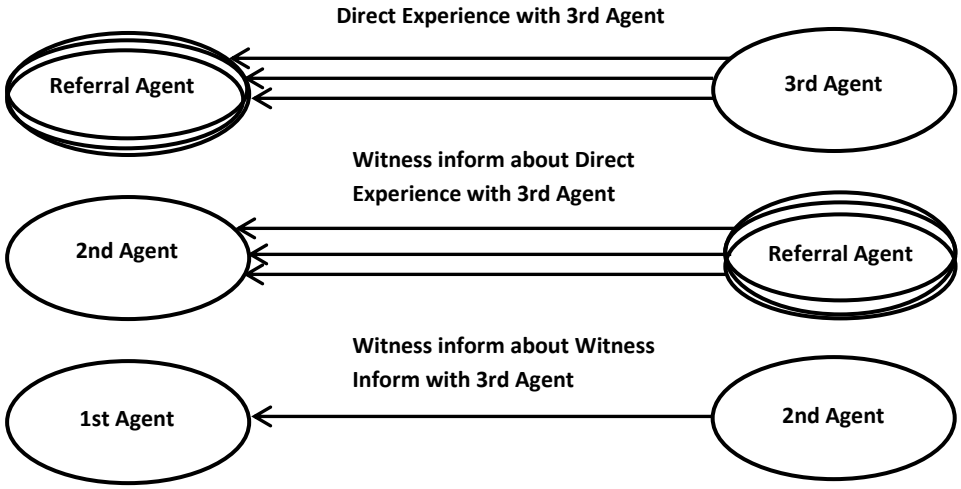

Figura 6.2. Esquema de cómo se lleva a cabo la comunicación incluyendo Agentes de Referencia

En la mayoría de los modelos de confianza, cuando los agentes tienen que decidir compartir su información con otros agentes, lo hacen teniendo en cuenta la reputación de estos agentes a la hora de aceptar o rechazar una determinada solicitud de información.

Nuestro enfoque parte de la suposición de que nuestro sistema de agentes actúa como una sociedad abierta, que incluiría algunos agentes a los que consideramos como agentes que no nos ofrecen confianza para compartir con ellos nuestra información personal. Con el fin de definir los niveles o condiciones de protección de la privacidad de nuestra información personal en los modelos de confianza, es necesario identificar (de acuerdo con la Regulación General de Protección de Datos), las condiciones legales que tienen que satisfacer los agentes de nuestro modelo de confianza en sus comunicaciones, para proteger nuestra privacidad.

6.3. PRIVACIDAD DE LA COMUNICACIÓN ENTRE AGENTES

Como hemos descrito en el modelo conceptual de privacidad en AmI (capítulo anterior), para preservar el derecho de protección de nuestra información personal, hay que tener en cuenta los diferentes niveles de protección de los datos que han sido establecidos de acuerdo a la normativa legal (cumplimiento normativa legal que regula la Protección de los Datos en la Unión Europea, *[Regulation EU, 2016/679]*. Teniendo esto en cuenta, las políticas de privacidad que deben cumplir los modelos de confianza incluyen la protección de la privacidad en los siguientes niveles: acceso a los datos, responsabilidades, localización de los datos, distribución de los datos, recuperación de los datos, soporte técnico a actividades ilegales.

Considerando estos niveles de protección de la privacidad, las comunicaciones entre los agentes participantes de nuestro modelo de confianza, deben garantizar (dese el punto de vista legal) el cumplimento de los siguientes derechos de privacidad:

1. Los agentes participantes han de ser informados de que otros agentes desean adquirir información personal sobre ellos (opiniones de confianza).

2. Los agentes participantes tienen que saber el nombre de los agentes que desean adquirir su información personal, la forma en la que lo van a hacer, y a qué agentes pueden transferir dicha información. Los agentes participantes deben recibir todo este tipo de información, sin importar, si la información ha sido obtenida de forma directa o indirecta por los agentes.

3. Los agentes participantes están autorizados a preguntar a otros agentes, si éstos se encuentran procesando algún tipo de información personal sobre ellos.

4. Los agentes participantes están autorizados a recibir una copia de su información personal de una manera comprensible.

5. Los agentes participantes están autorizados a solicitar o preguntar acerca de la pérdida, bloqueo o eliminación de los datos.

6. Teniendo en cuenta que las decisiones basadas en la información personal pueden afectar directamente a otros agentes, los agentes participantes deben adoptar medidas de seguridad adecuadas, como puede ser ofreciendo la oportunidad de analizar la opinión que hay detrás de ellos (por ejemplo, discutiendo o rechazando decisiones basadas en información incorrecta).

Para integrar la protección de estos seis derechos de privacidad en las comunicaciones entre los agentes que ejecutan un modelo de confianza, hemos incluido en los protocolos de las relaciones de confianza propios del entorno de experimentación ART testbed, el intercambio de mensajes adicionales, los cuales actúan como mecanismos de control, permitiendo así a los agentes que han de confiar en otros agentes satisfacer estos derechos derivados de la Regulación General de Protección de Datos de la Unión Europea.

Los mensajes de comunicación adicionales intercambiados por los agentes, que se han propuesto son:

1. Un único mensaje de comunicación. Este mensaje único informará a cada “3rd Agent” sobre la futura adquisición de opiniones sobre él, y sobre qué opiniones han sido utilizadas.

   Utilizando este tipo de mensaje un agente puede cumplir con el primer derecho de privacidad establecido: estar informado cuando otros agentes estén recogiendo información sobre él.

2. Una pareja de mensajes adicionales. Estos mensajes corresponden a un protocolo de negociación (una oferta o propuesta, seguida de una contraoferta), sobre quién puede transmitir las opiniones (el agente que hemos llamado “1st Agent”).

Aunque los agentes que recogen la información (labor de nuestro “2nd Agent”), envían una propuesta inicial (a todos los agentes, a una posible lista de “1st Agent” o a ninguno) acerca de dos maneras de transmitir las opiniones (directa o indirecta); la decisión final tiene que corresponder al “3rd Agent”, tanto si acepta como si ignora la propuesta realizada por el “2nd Agent”.

Adicionalmente, hemos definido una restricción de la privacidad para cada “1st Agent”, con el fin de evitar la posibilidad de que se revelen las opiniones de forma involuntaria, siguiendo la similitud de las políticas de seguridad aplicadas en la comunicación. De esta forma, la correspondiente decisión final toma la forma de una declaración (“statement”) de privacidad.

Utilizando este protocolo de negociación, el segundo derecho de privacidad que hemos establecido puede cumplirse: un agente puede restringir con quién difunde su información personal, y el modo en el que lo hace, bajo la declaración de las políticas de seguridad a seguir en el “statement”.

3. Los agentes que actúan como “3rd Agent” solicitarán a cualquier otro tipo de agentes (“1st Agent”) si éstos se encuentran adquiriendo información sobre ellos, y de qué información se trata. Esto implica dos mensajes: uno solicitando la información, y el otro dando la respuesta.

   El tercer derecho de privacidad se puede alcanzar mediante el correcto uso de este intercambio de mensajes, en el que un agente solicita a otros si están adquiriendo información sobre ellos o no.

4. Un único mensaje de comunicación. Este mensaje único ordenará la eliminación o bloqueo de todas las opiniones que han sido ya adquiridas.

   Este mensaje permite el cumplimiento del quinto derecho de privacidad, por el cual los agentes pueden pedir a otros, la eliminación o bloqueo de cualquier tipo de información sobre ellos.

5. Un diálogo argumentado entre el “2nd Agent” y “3rd Agent” sobre las razones que hay detrás de la adquisición y transmisión de las opiniones, teniendo en cuenta una supuesta inexactitud o imprecisión de las mismas. Cada argumento puede incluir el intercambio de varios mensajes, que tienen en cuenta los diferentes factores involucrados en este tipo de opiniones.

   Esta secuencia de mensajes puede terminar en un acuerdo final (uno de los agentes reconoce y acepta las razones del otro agente), o puede terminar en desacuerdo; este tipo de desacuerdo puede ser dirigido por un “3rd Agent" que será el agente que decida el bloqueo o eliminación de la comunicación de este tipo de opiniones.

   Este diálogo argumentado permite a los agentes cumplir con los definidos como cuarto y sexto derecho de privacidad. Un agente puede obtener la información adquirida sobre él (cuarto derecho de privacidad), y puede también tratar o analizar las razones que sustentan las opiniones emitidas sobre él (sexto derecho de privacidad).

En la figura presentada a continuación aparecen definidos los derechos de privacidad que deben cumplir los agentes de confianza en sus comunicaciones, así como los correspondientes mensajes adicionales que deben intercambiar entre ellos para la protección de los mismos.

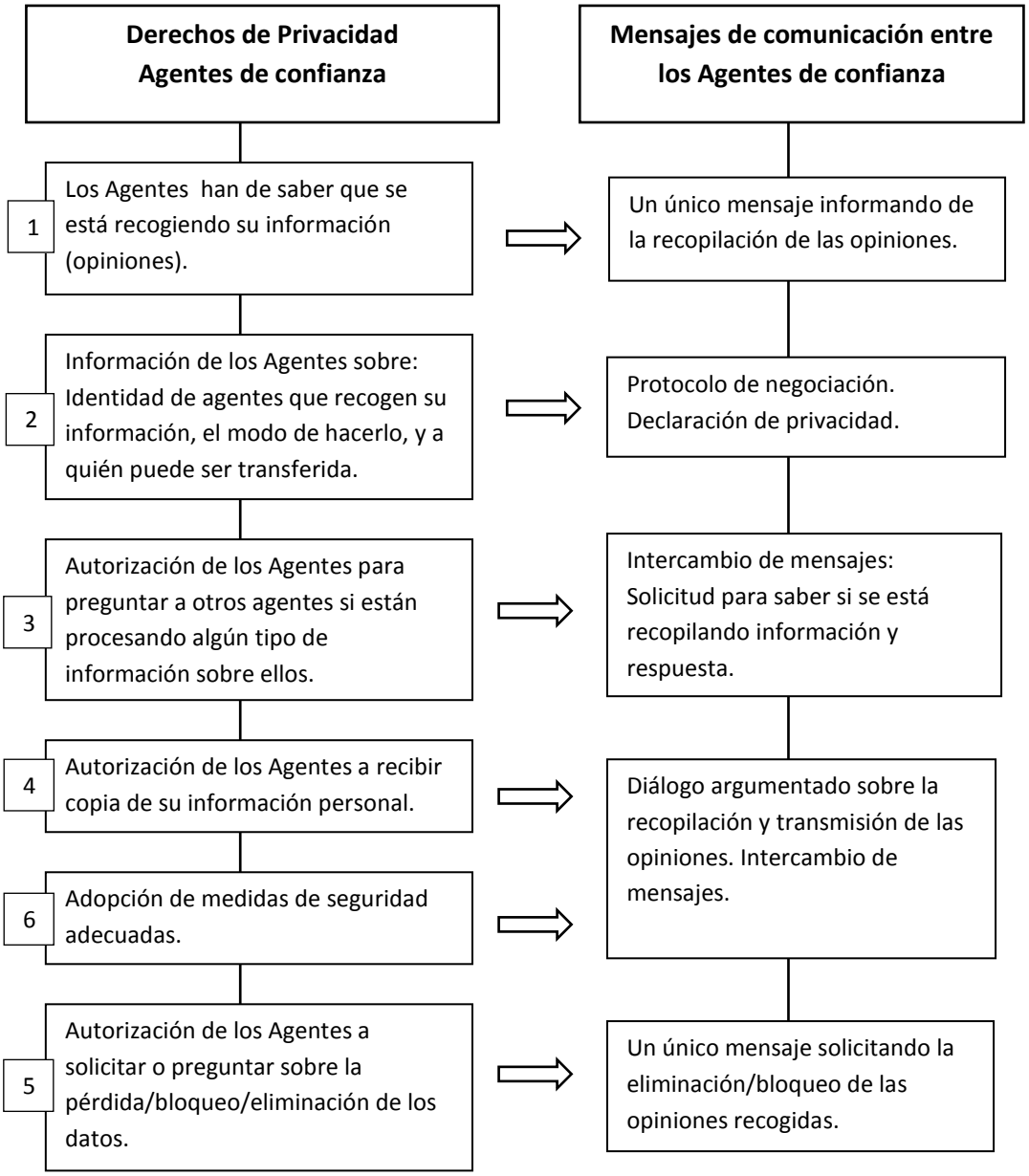

Figura 6.3. Protección de la Privacidad de la Comunicación entre los Agentes de confianza

Teniendo en cuenta que este intercambio de mensajes puede tener lugar o no en la comunicación de los agentes del modelo de confianza, se ha considerado necesario definir las posibles infracciones de privacidad que pueden darse, con el fin de verificar el cumplimiento legal de los derechos de privacidad que han sido establecidos.

Estas infracciones de privacidad han sido expresadas de la siguiente forma:

1. Un “1st/2nd Agent” adquiere las opiniones sobre otro agente, sin su conocimiento (no se ha enviado ningún mensaje previo informando de esta acción).

2. Un “2nd Agent” envía las opiniones sobre un “3rd Agent” al “1st Agent”, las cuales no estaban incluidas en la correspondiente declaración de privacidad del “3rd Agent”.

3. Un “2nd Agent” que ha sido informado con opiniones incompletas o incorrectas sobre un 3rd Agent”, envía una serie de opiniones diferentes o más ampliadas sobre él al “1st Agent”.

4. Un “1st/2nd Agent” que ignora la orden de bloquear o eliminar las opiniones adquiridas, y sigue transmitiendo dicha información.

5. Un “1st/2nd Agent” que no explica el motivo por el que las opiniones sobre un “3rd Agent” están siendo difundidas, es decir, no responde a la petición de justificación del “3rd Agent”.

6. Posibilidad de que los agentes rompan la seguridad de las comunicaciones donde las opiniones han sido difundidas: un “1st Agent” transmitiendo las opiniones sobre un “3rd Agent”, sin que la adquisición de las mismas haya sido realizada con una aprobación previa (directa o indirectamente) por parte de ningún “2nd/3rd Agent”.

Para verificar el cumplimiento legal de los derechos de privacidad establecidos en el intercambio de mensajes entre los agentes, hemos considerado necesario formalizar explícitamente este conjunto de restricciones o infracciones de privacidad, que pueden tener lugar en la comunicación de los agentes. La especificación de estas normas, y sus correspondientes consecuencias serán implementadas de manera automática a través de una Institución Electrónica.

Estas organizaciones velan por el control social del comportamiento de los agentes, definiendo las desviaciones del entendido como comportamiento correcto de esa sociedad de agentes, y estableciendo penalizaciones a los agentes cuyo comportamiento no sea socialmente aceptable.

6.4. PROTOCOLOS DE PROTECCIÓN DE LA PRIVACIDAD EN EL DOMINIO ART (Agent Reputation and Trust)

Para implementar los mensajes de comunicación entre los agentes de confianza, y poder así cumplir con los derechos de privacidad que han sido establecidos, hemos elegido, como se ha comentado anteriormente, el entorno de experimentación del ART testbed (Agent Reputation and Trust), *[K. Fullam, et al. 2005]*. Algunos de los agentes participantes de esta sociedad actúan como tasadores de cuadros, por lo que podemos incluirlos dentro del dominio de aplicación de la Inteligencia Ambiental relacionado con el Comercio/Negocios, en el que hemos considerado que el nivel de protección de la información de los usuarios es bajo (capítulo 5).

En este dominio de tasación de cuadros correspondiente al ART testbed, cada agente recibe una colección de cuadros pertenecientes a cualquier época (en la que puede no ser un experto) para evaluarlos, dentro de una entidad que simula a los autores de los cuadros. Por ello, cada agente va a necesitar la cooperación de otros agentes en la tasación de los cuadros que pertenecen a épocas en las que no son expertos. Teniendo en cuenta que la experiencia de cada agente en cada época es desconocida inicialmente, los agentes necesitan conocerla y ganarse su confianza, para conseguir la cooperación de otros agentes. Esta tarea se convierte en el verdadero objetivo de la estrategia de los agentes en el entorno del ART testbed. Además, cada agente va a decidir quiénes son los agentes que le interesa tener como socios; y esta decisión la lleva a cabo atendiendo a los siguientes criterios: que muestren una actitud sincera y cooperativa, que tengan conocimiento valioso acerca de los demás agentes, y que cuenten con experiencia en las diferentes épocas de la pintura.

Para establecer las locuciones, roles y relaciones que tienen lugar en las interacciones del dominio del arte correspondiente al ART, se ha utilizado la plataforma del banco de pruebas del ART implementado en el entorno de JADE *[J. Moya and J. Carbo, 2012]*; los cuales se corresponden con los protocolos involucrados en el dominio de pruebas del ART, formalizados siguiendo el estándar FIPA (Foundation for Intelligent Physical Agents) en los trabajos presentados en *[J. Carbo and J.M. Molina, 2009]*.

En resumen, hemos utilizado el dominio de aplicación del ART para definir los mensajes adicionales que resultan necesarios atendiendo a los requerimientos de privacidad establecidos (derechos de privacidad), y que se corresponden con los cinco tipos de mensajes de comunicación entre agentes, definidos en el apartado anterior. Estos mensajes incluyen los correspondientes conceptos, predicados y acciones, necesarios para definir el contenido de los mensajes intercambiados entre los agentes.

Estos mensajes o protocolos de comunicación entre los agentes, que dan cumplimiento a los seis derechos de privacidad establecidos (en conformidad con FIPA), aplicados al banco de pruebas del dominio del ART e implementados en JADE *[F.L. Bellifemine, et al. 2007]*, son los siguientes:

- *Protocolo 1***.** Un mensaje (1) que tiene asociada la intencionalidad ("performative") de INFORM (correspondiente al conjunto de actos comunicativos que FIPA determina que deben ir asociados a cada mensaje), y con predicado *"IsCollecting"* como contenido, perteneciente a la ontología definida para JADE *[J, Moya and J. Carbo, 2012]*. Este tipo de predicado tiene las siguientes propiedades relacionadas con los siguientes conceptos como valores:

  Who: Agente Tasador

  On: Época

  Value: Reputación

- *Protocolo 2*. Una pareja de mensajes: el primero (2a) con PROPOSE como intencionalidad asociada, y un predicado *"StatesPrivacy"* como contenido. Este predicado presenta las siguientes propiedades relacionadas con los siguientes conceptos como valores:

  Who: Agente Tasador

  On: Época

  Whom: Nadie/Todos/Agente Tasador

  Type: Nivel Indiferente

  How: Políticas de Seguridad

  El concepto de Nivel Indiferente presenta dos valores: directo (información obtenida de las experiencias directas), e Indirecto (información declarada).
  En cuanto a las Políticas de Seguridad, éstas describirían las reglas que deben aplicarse en los algoritmos criptográficos de las comunicaciones.

  El segundo mensaje (2b) es la respuesta correspondiente al primer mensaje PROPOSE. Esta respuesta puede ser ACCEPT PROPOSAL, o REJECT PROPOSAL. En el caso en el que se rechace la propuesta, el mensaje incluiría un predicado *"StatesPrivacy"* como contenido, con el objetivo de que sea considerada una contrapropuesta.

- *Protocolo 3*. Una pareja de mensajes: el primero (3a) con intención QUERY-REF (FIPA), un predicado *"Is Collecting"* como contenido, y en el que la característica valor presenta un concepto vacío asociado. El segundo mensaje (3b) es la respuesta INFORM-REF con el predicado *"Is Collecting"* como contenido, que cumple con la reputación obtenida.

- *Protocolo 4*. Una pareja de mensajes: el primero (4a) con intención REQUEST (FIPA), y con predicado *"Blocking or Deleting"* como contenido. Este predicado presenta los siguientes conceptos como valores:

  Who: Agente Tasador

  On: Época

  Value: Reputación

  A continuación, el otro agente tiene que dar como respuesta un mensaje con intención AGREE (4b).

- *Protocolo 5*. Una secuencia de mensajes: el primer mensaje (5a) de un agente inicial con QUERY-REF como especificación FIPA, y un predicado *"Justification"* como contenido, que tiene las siguientes propiedades, y sus correspondientes conceptos como valores:

  Who: Agente Tasador

  On: Época

  Value: Reputación

  From: Agente Tasador

  Type: Indirection Level

  Initial Value

  Las propiedades From, Type e Initial Value tienen un concepto vacío asociado, que se corresponde con el segundo mensaje de respuesta (5b) INFORM-REF, que cumpliría con el agente fuente de cada valor de reputación defendido, el modo en el que el valor de la reputación ha sido obtenido (direct versus indirect), y el valor original enviado por este agente fuente.

  Después de este segundo mensaje, un mensaje adicional REQUEST (5c) puede tener lugar desde el agente inicial, para sugerir a otros agentes que rectifiquen el valor de la reputación obtenida del agente fuente. Con el fin de motivar este tipo de rectificación, el agente iniciador incluiría las especificaciones de la interacción directa con este agente fuente (siempre y cuando esta interacción tenga lugar realmente).

Este mensaje REQUEST, incluye un predicado *"Rectifying"* que contiene el verdadero valor de tasación del cuadro correspondiente a esta interacción. Para finalizar, otro agente podría contestar con un mensaje REFUSE o AGREE (5d).

En la siguiente figura, aparecen representados estos cinco protocolos que hemos definido:

Figura 6.4. Protocolos de protección de la Privacidad en JADE en el dominio del ART

6.5. CASO DE ESTUDIO Y APLICACIÓN DEL MODELO

Una vez que han sido aplicados los mensajes adicionales intercambiados entre los agentes en el dominio de aplicación del ART, cumpliendo así con los requerimientos de privacidad que hemos establecido (derechos de privacidad), vamos a definir a continuación la manera en la que se decide cuáles son los agentes merecedores de compartir con ellos nuestras opiniones privadas.

Este razonamiento interno de los agentes de confianza es ligeramente distinto de la mayoría de los sistemas utilizados para evaluar la confianza, ya que lo que vamos a decidir es si un agente es capaz de preservar la privacidad de nuestras opiniones o no, con otro agente, en lugar de decidir cuánto confiamos en ese agente en particular. La decisión se convierte así, en una "línea roja" que debe ser mantenida durante todo el proceso, aunque las decisiones de confianza normales suelen darse en un momento determinado, cambiando de forma dinámica dependiendo de los valores de reputación, que varían según el comportamiento en curso del agente en quien confiar.

Se necesita por tanto establecer, cuáles son las decisiones que deben tomar los agentes en sus comunicaciones para proteger nuestras opiniones privadas. Es decir, queremos saber a qué agentes vetamos el acceso a las opiniones privadas que compartimos y a cuáles no. Se trata pues de establecer una decisión binaria, ya que lo que decidimos es si confiamos o no en un agente determinado a la hora de compartir o no nuestras opiniones privadas (no importa en este caso, cuánto confiemos en ese agente).

En una situación normal, tendríamos un número de agentes (posiblemente extenso) solicitándonos permiso para acceder a nuestra información (protocolo 1 de privacidad), una declaración de privacidad registrada sobre la obtención de nuestras opiniones (protocolo 2 de privacidad), y la consiguiente opinión difundida sobre nosotros (nuestra reputación). Teniendo en cuenta que a priori, no disponemos de ningún tipo de información sobre estos agentes, vamos a asumir que son honestos.

Tras producirse el intercambio de los mensajes iniciales, los agentes comienzan a funcionar como modelos de confianza en un dominio de aplicación determinado. La decisión fundamental que deben tomar los agentes, atendiendo a la protección de la privacidad, consiste en decidir si se debe iniciar o no el protocolo 4 de privacidad *(Blocking/Deleting Request)* o el protocolo 5 *(Justification Query)*, que tendrán lugar cuando las opiniones de los agentes se vuelven perjudiciales para nosotros, o difieren bastante de lo que se esperaba.

Teniendo en cuenta estas consideraciones y con el fin de decidir quiénes son los agentes a los que vamos a restringir (vetar) el acceso a nuestras opiniones privadas, esta situación general planteada en la que intervienen "n" agentes, ha sido simplificada a un caso particular de dos agentes, donde tendremos que decidir cuál de ellos es de confianza, y por tanto merecedor de compartir nuestras opiniones privadas.

6.5.1. Conceptualización del modelo

Para aplicar nuestro modelo de Privacidad Digital en AmI, hemos utilizado los datos de la competición internacional del ART testbed, que tuvo lugar en el año 2007 en el marco de la conferencia AAMAS de ese año *[Competition of ART testbed, 2007]*. El data set utilizado consta de una colección de 57 cuadros en el que se comparan las opiniones de tres Agentes: UNO, ZeCarioca y AFRASArt *[UNO], [ZeCarioca], [AFRASArt]* sobre cada cuadro, con la estimación final (disponemos de 228 instancias). Hemos tomado el papel de agente IAM *[IAM]* (ganador de dicha competición), y como agentes que evalúan nuestra preocupación sobre la privacidad, los agentes ZeCarioca y UNO, para todos los cuadros que han sido tasados en esta competición.

La diferencia entre las opiniones de estos dos agentes con la estimación final de cada cuadro (que es el valor objetivo), va a ser la clave que nos ayudará a decidir qué agentes no son "de fiar" para nosotros (como Agentes IAM), con el objetivo de restringir completamente el acceso a nuestra información personal a estos agentes, y como estamos en una competición, perjudicaríamos sus posibilidades de ganar.

El modelo presentado, nos va a permitir predecir la categoría de las instancias (porcentaje de aciertos del clasificador), en función de una serie de atributos de entrada. Para ello, hemos implementado los razonamientos internos de cada agente utilizando distintos algoritmos de clasificación, utilizando como herramienta de minería de datos *Waikato Environment for Knowledge Analysis [WEKA, v.3.6.1.].* Las opiniones de los Agentes ZeCarioca y UNO sobre los cuadros van a ser los atributos de entrada, junto con la estimación final de cada cuadro (Final Estimation Agent), mientras que la salida de nuestros algoritmos de clasificación será la decisión final de privacidad que tomemos de ambos agentes (si compartimos o no nuestras opiniones privadas con ellos).

Nuestro modelo, por lo tanto consta de cuatro atributos de entrada numéricos, cuyos valores han sido tomados en un intervalo discreto que representará los valores de cada clase. Estos atributos son: ZeCarioca, UNO, Estimación Final de los cuadros, y CLASE que representa el atributo que hay que predecir por nuestros algoritmos de clasificación. Este cuarto atributo, CLASE se encuentra definido en el intervalo {0,1}.

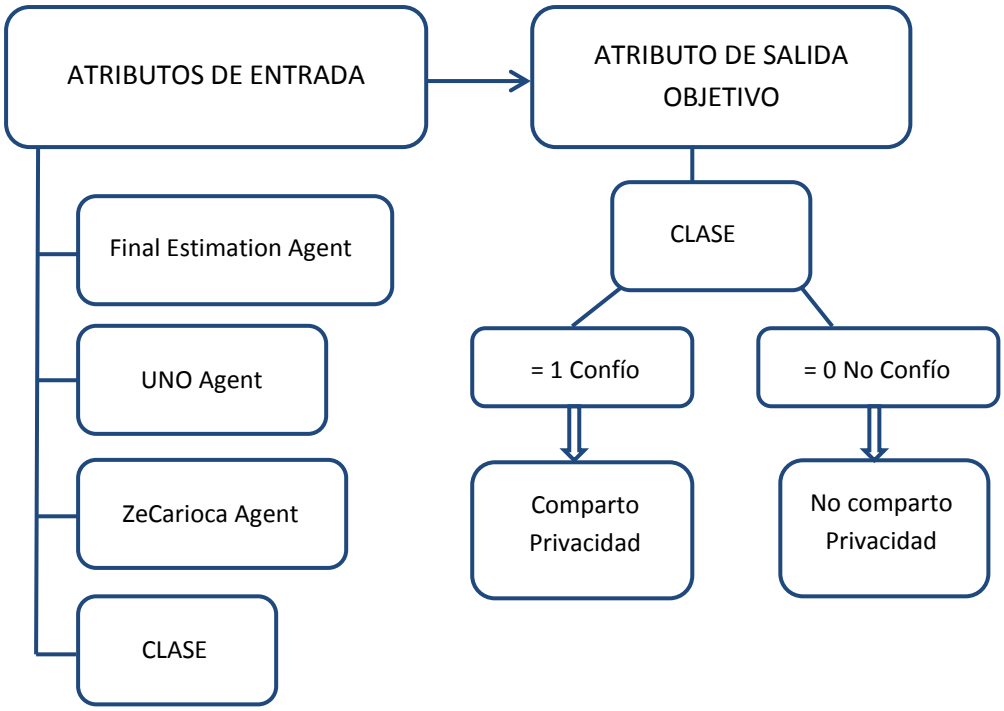

Figura 6.5. Atributos del modelo de privacidad digital en WEKA

Agente Final Estimation Agent: agente que representa la estimación final.

Agentes UNO y ZeCarioca: agentes que evalúan nuestra preocupación sobre la privacidad.

El atributo CLASE va a ser nuestra variable objetivo que hay que predecir, y como hemos dicho que se trata de una decisión binaria, presenta dos valores {1,0}:

CLASE = 1 (Valor del agente que está más próximo al valor del Final Estimation Agent). Este resultado indica que confío en este agente, por lo que compartiré con él mis opiniones privadas.

CLASE = 0 (Valor del agente más alejado del valor del Final Estimation Agent). Este resultado indica que no confío en este agente, por lo que no compartiré con él mis opiniones privadas.

6.5.2. Validación del modelo

Para implementar el modelo, se ha utilizado el entorno de análisis y evaluación de técnicas de aprendizaje la aplicación WEKA (v.3.6.1.), con la que hemos llevado a cabo las tareas de clasificación considerando diferente número de cuadros; lo cual nos ha permitido saber si el tamaño de cada ventana influye en la decisión final. Es de suponer que si consideramos un tamaño de ventana pequeño (con un número bajo de cuadros), la clasificación será más eficaz pero menos acertada, mientras que después de considerar un gran número de cuadros teniendo en cuenta el acierto, es de esperar que la exactitud se vuelva más o menos estable. En base a la clasificación realizada, vamos a predecir la categoría de las instancias (porcentaje de aciertos del clasificador), en función de los atributos de entrada establecidos.

Como se ha indicado, nuestro data set consta de una serie de 57 cuadros y 228 instancias (comparaciones de las opiniones de los Agentes sobre cada cuadro con la Estimación Final de los cuadros). Las opiniones de los Agentes ZeCarioca y UNO sobre los cuadros van a ser nuestros atributos de entrada, junto con el Final Estimation Agent de cada cuadro, mientras que la salida, que va a ser nuestro objetivo, CLASE, será la decisión final de privacidad de ambos agentes, que nos ayudará a elegir con qué agente compartimos nuestras opiniones privadas y con cuál no.

Para elegir el método de evaluación del clasificador y poder comparar así nuestra CLASE objetivo, con las clases reales de todas las instancias, se probó con distintas opciones que presenta WEKA: Use Training Set, Supplied Test Set, Percentage Split, Cross-Validation. El método Cross-Validation permite dividir las instancias en tantas carpetas como indique el parámetro, y en cada evaluación se toman las instancias de cada carpeta como datos de test, tomándose el resto de datos como datos de entrenamiento, siendo los errores calculados el promedio de todas las ejecuciones. Aunque como vemos, el Cross-Validation es el método más elaborado y costoso, es el que se eligió como método de evaluación, ya que fue con el que mayor número de aciertos se obtuvo.

El entrenamiento del Cross-Validation se llevó a cabo utilizando los cuadros que el Agente IAM solicitó que evaluaran los Agentes ZeCarioca y UNO, junto con la estimación final de los correspondientes cuadros predicha por el Agente IAM en el juego de competición del ART Testbed, 2007. En nuestro caso, el Agente que se excluye para compartir nuestra información personal (opiniones privadas), sería el considerado incompetente por nuestro Agente IAM, que determina esta condición, teniendo en cuenta la diferencia entre la evaluación realizada y la estimación final considerada para cada cuadro.

A continuación, se prepararon tres tipos de escenarios con diferentes números de valoraciones (opiniones) sobre los cuadros:

- Escenario 1: consta de 4 atributos (Final Estimation Agent, UNO, ZeCarioca, y CLASE). Este primer escenario consta de 57 filas y 228 instancias.
- Escenario 2: consta de 7 atributos (Final Estimation Agent/UNO/ZeCarioca/Final Estimation Agent/UNO/ZeCarioca/CLASE. Este escenario se compone de 56 filas y 392 instancias.
- Escenario 3: consta de 10 atributos (Final Estimation Agent/UNO/ZeCarioca/Final Estimation Agent/UNO/ZeCarioca/Final Estimation Agent/UNO/ZeCarioca/CLASE. Este último escenario consta de 54 filas y 540 instancias.

Setting 1 = Window size 4 (57 rows, 228 instances)

Setting 2 = Window size 7 (56 rows, 392 instances)

Setting 3 = Window size 10 (54 rows, 540 instances)

Figura 6.6. Tipos de escenarios propuestos para compartir nuestras opiniones privadas

Considerando estos tres tipos de escenarios, se aplicaron diferentes algoritmos de clasificación, con el fin de obtener el número de instancias clasificadas correctamente, de acuerdo a nuestra CLASE objetivo. Los algoritmos de clasificación utilizados fueron: MLP, J48, RBF Network, PART, RIDOR, OneR, y TreesLMT:

- MLP (Multilayer Perception): clasificación mediante la utilización de funciones.
- J48 (Implementación del C4.5): clasificación mediante árboles de decisión (nivel de confianza).
- RBF Network (Radial Basis Function Network): clasificación mediante la utilización de funciones.
- PART: clasificación mediante reglas de decisión a partir de árboles de decisión parcialmente podados.
- RIDOR (Ripple Down Rule): clasificación mediante reglas de decisión.
- OneR: clasificación mediante reglas de decisión, selecciona el atributo que mejor "explica" la clase objetivo, el que presenta un error mínimo en la predicción.
- TreesLMT (Logistic Model Trees): clasificación mediante árboles de decisión.

6.5.3. Resultados obtenidos

A continuación se presentan los resultados obtenidos en WEKA, al aplicar los algoritmos de clasificación indicados, y teniendo en cuenta los tres tipos de escenarios establecidos.

Los resultados obtenidos nos muestran el porcentaje de aciertos de cada clasificador, teniendo en cuenta los tres tamaños de ventana escogidos, al comparar las opiniones (estimaciones) de los Agentes UNO y ZeCarioca, junto al Agente de Estimación Final, que nos mostrará nuestro objetivo, atributo CLASE. Este atributo

objetivo, CLASE representa la decisión final que tomaremos para elegir el agente confiable, con el que compartiremos nuestras opiniones privadas.

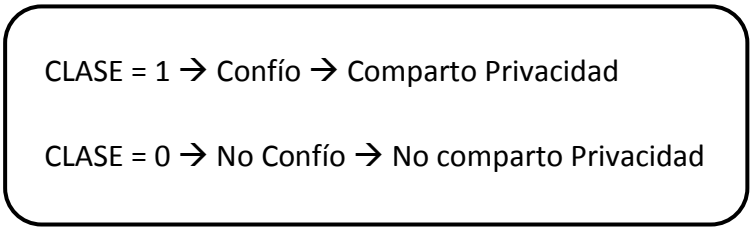

Figura 6.7. Decisión final para compartir nuestras opiniones privadas

Classifier	**Window size 4**	**Window size 7**	**Window size 10**
MLP	70,175	55,357	60,377
J48	54,386	64,285	56,603
RBF Network	68,421	58,928	49,056
PART	54,386	58,928	50,943
RIDOR	56,140	62,500	56,603
OneR	61,403	58,928	54,717
TreesLMT	61,403	55,357	52,830

Tabla 6.1. Valores del porcentaje de aciertos por clasificador en los tres tipos de escenarios

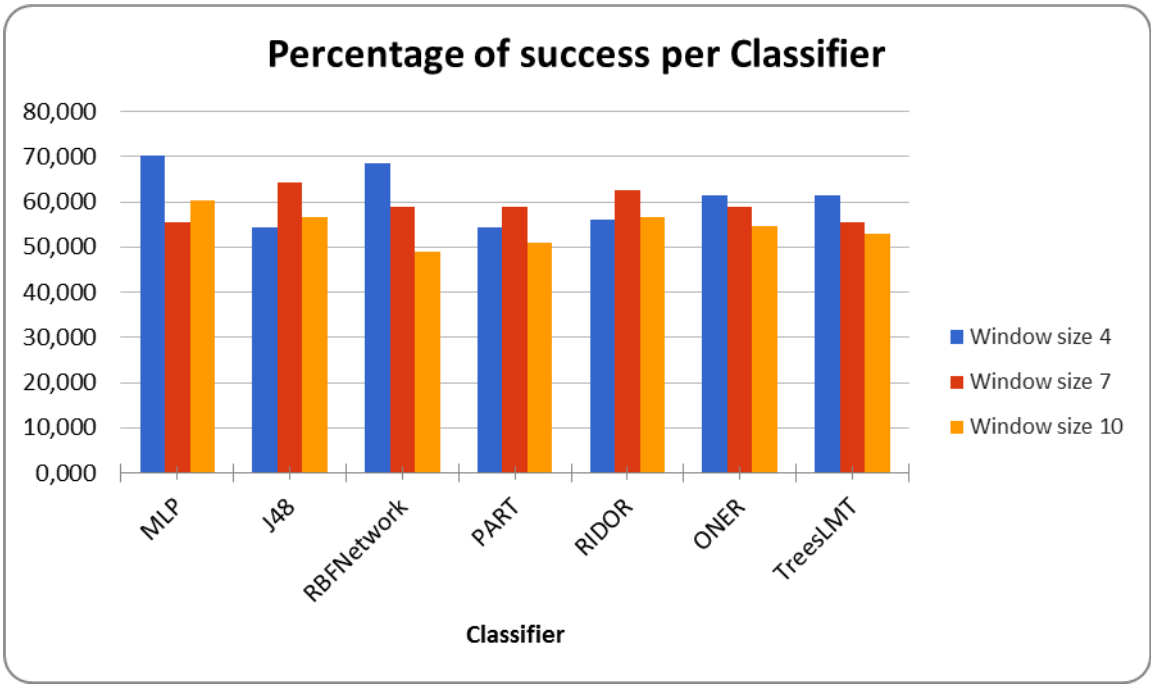

Figura 6.8. Diagrama de barras, porcentaje de aciertos de los clasificadores para decidir el agente en el que confiamos para compartir nuestras opiniones privadas

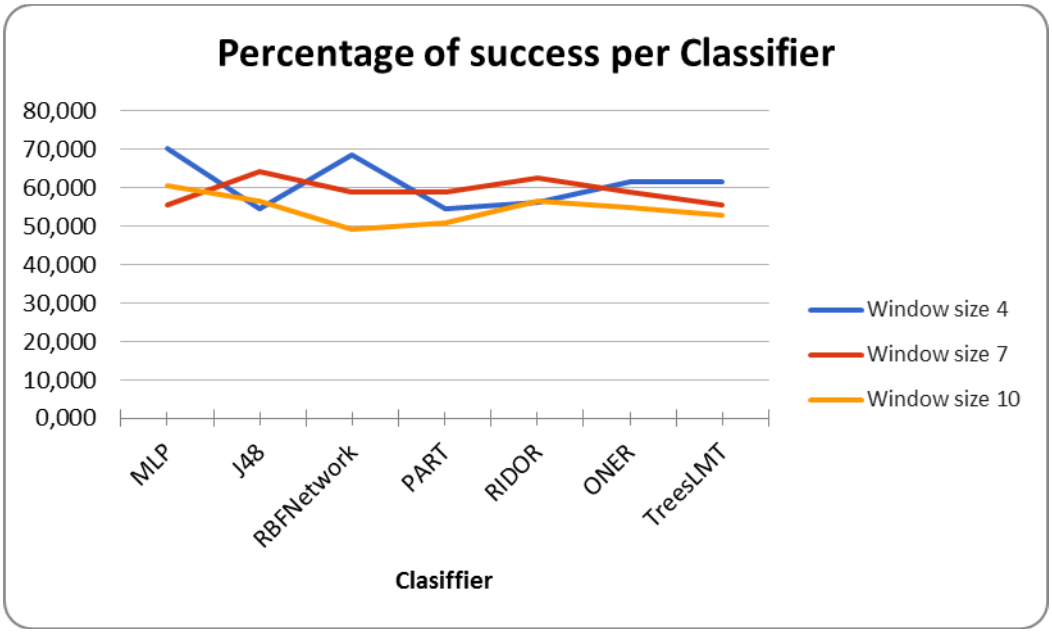

Figura 6.9. Diagrama de líneas, porcentaje de aciertos de los clasificadores para decidir el agente en el que confiamos para compartir nuestras opiniones privadas

A la vista de los resultados mostrados, no podemos concluir que el hecho de considerar un número de evaluaciones alto en la tasación de los cuadros, mejore las decisiones para compartir nuestras opiniones privadas, ya los tamaños de ventana más pequeños (window size 4, window size 7) son los que han ofrecido los resultados más satisfactorios (70,17%, 68,42%, 64,28% y 62,50%).

Por otra parte, observamos que considerando el escenario 1, tamaño de ventana menor (window size 4) es con el que se han producido los valores más altos de acierto (70,17% y 68,42%), aunque también se observa que es el escenario que presenta más fluctuaciones de acierto según el clasificador considerado. En este escenario, los valores de aciertos se encuentran comprendidos entre el 54,38 y el 70,17% (valor más alto obtenido).

El segundo escenario considerado, (window size 7) es el que presenta menor fluctuación en los valores de aciertos, estando estos valores comprendidos entre el 55,35 y el 64,28%.

Con el escenario con mayor número de atributos e instancias, (window 10), los resultados obtenidos representan una fluctuación intermedia entre los dos escenarios anteriores, estando los valores obtenidos comprendidos entre el 49,05 (valor más bajo obtenido), y el 60,37%.

Los valores más altos de aciertos del clasificador que representan la decisión de confiar o no en un agente, y así compartir con él nuestras opiniones privadas, corresponden a valores comprendidos entre el 68,42 y el 70,17%, por lo que un 30% de las evaluaciones no nos ayudan a decidir si confiamos o no.

Para terminar, otra consideración que queremos indicar es que utilizando WEKA como técnica de análisis y evaluación de aprendizaje automático, no se puede determinar si el tamaño de la ventana influye en la toma de decisiones sobre la confianza, ya que a la vista de los resultados comentados, un número alto de opiniones no siempre mejora los valores de aciertos obtenidos.

6.5.4. Consecuencias sobre las infracciones de privacidad

Una vez implementada la manera en la que decidiremos con quién compartimos nuestras opiniones privadas, y con el fin de controlar el cumplimiento de los derechos de privacidad que se han establecido, se han formalizado las posibles infracciones sobre estos derechos junto con sus correspondientes sanciones utilizando la Institución Electrónica "Islander" *[M. Esteva, et al. 2002]*, como herramienta de especificación de las normas y sanciones correspondientes que deben cumplir los agentes.

Se ha optado por "Islander" porque diseña cada restricción como una combinación de elementos de texto y gráficos, que resulta muy intuitiva, y porque no asume ningún tipo de arquitectura o lenguaje particular entre los agentes participantes.

Recordemos las seis infracciones de privacidad que hemos establecido:

1. Un "1st/2nd Agent" adquiere las opiniones sobre otro agente, sin su conocimiento (no se ha enviado ningún mensaje previo informando de esta acción).

2. Un "2nd Agent" envía las opiniones sobre un "3rd Agent" al "1st Agent" que no estaban incluidas en la correspondiente declaración de privacidad del "3rd Agent".

3. Un "2nd Agent" que ha sido informado con opiniones incompletas o incorrectas sobre un 3rd Agent", envía una serie de opiniones diferentes o más ampliadas sobre él al "1st Agent".

4. Un "1st/2nd Agent" que ignora la orden de bloquear o eliminar las opiniones adquiridas, y sigue transmitiendo dicha información.

5. Un "1st/2nd Agent" que no explica el motivo por el que las opiniones sobre un "3rd Agent" están siendo difundidas, es decir, no responde a la petición de justificación del "3rd Agent".

6. Posibilidad de que los agentes rompan la seguridad de las comunicaciones donde las opiniones han sido difundidas: un “1st Agent” transmitiendo las opiniones sobre un “3rd Agent”, sin que la adquisición de las mismas haya sido realizada con una aprobación previa (directa o indirectamente) por parte de ningún “2nd/3rd Agent”.

En la Institución Electrónica “Islander” cada escena (Scene) representa la interacción que tiene lugar entre los agentes participantes.

A continuación aparecen detalladas las cinco escenas utilizadas en “Islander”, que nos han servido para formalizar estas seis infracciones de privacidad.

1. Scene 1: Step 2b. Tiene lugar cuando el “Agent1” consulta al “Agent3” sobre la reputación acerca de la infracción cometida por el “Agent2”. Este paso ocurre en vez de la secuencia normal de los pasos 1-2a, en la que el “Agent1” informa previamente al “Agent2” sobre sus intenciones de recoger información sobre su reputación. El agente puede pasar por los estados “not informed”, “informed” y “queried”.

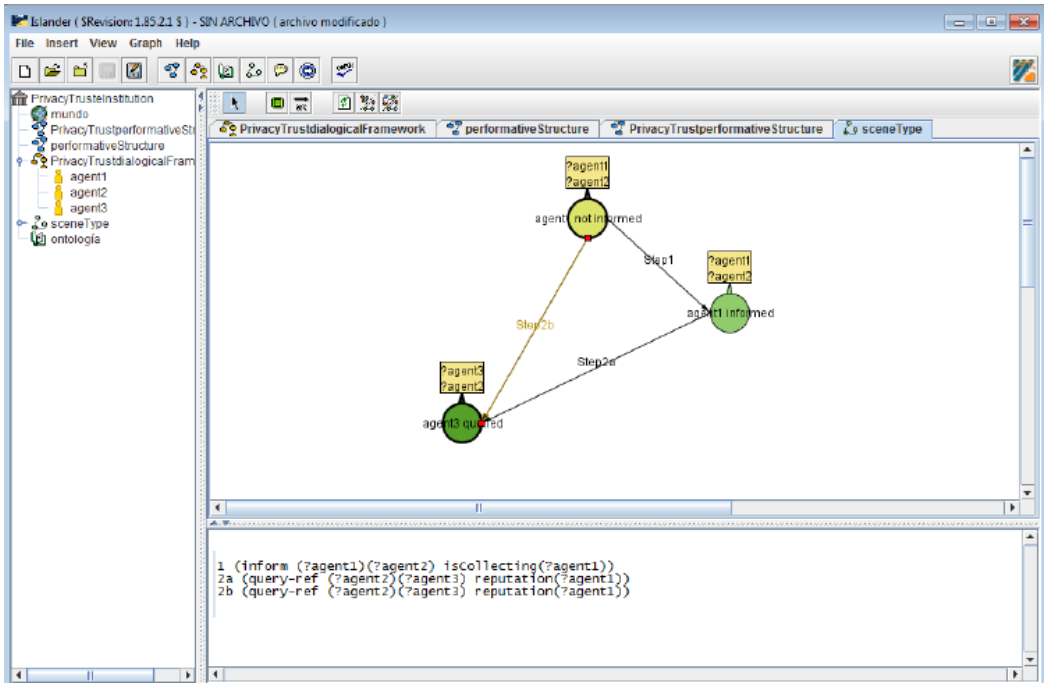

Figura 6.10. Captura de pantalla Islander, Scene 1

2. Scene 2: Steps 1-2. El “Agent2” acepta un acuerdo de privacidad con el “Agent1” que incluye no compartir la información sobre la reputación de este último con el “Agent3”. A continuación el “Agent3” solicita información sobre la reputación del “Agent1” (step 3), teniendo entonces lugar la infracción en la declaración de privacidad del “Agent2”, que está informando al “Agent3” sobre la reputación del “Agent1” (step 4). El agente pasa por los estados “no agreement”, “agreement”, “queried reputation” y “shared reputation”.

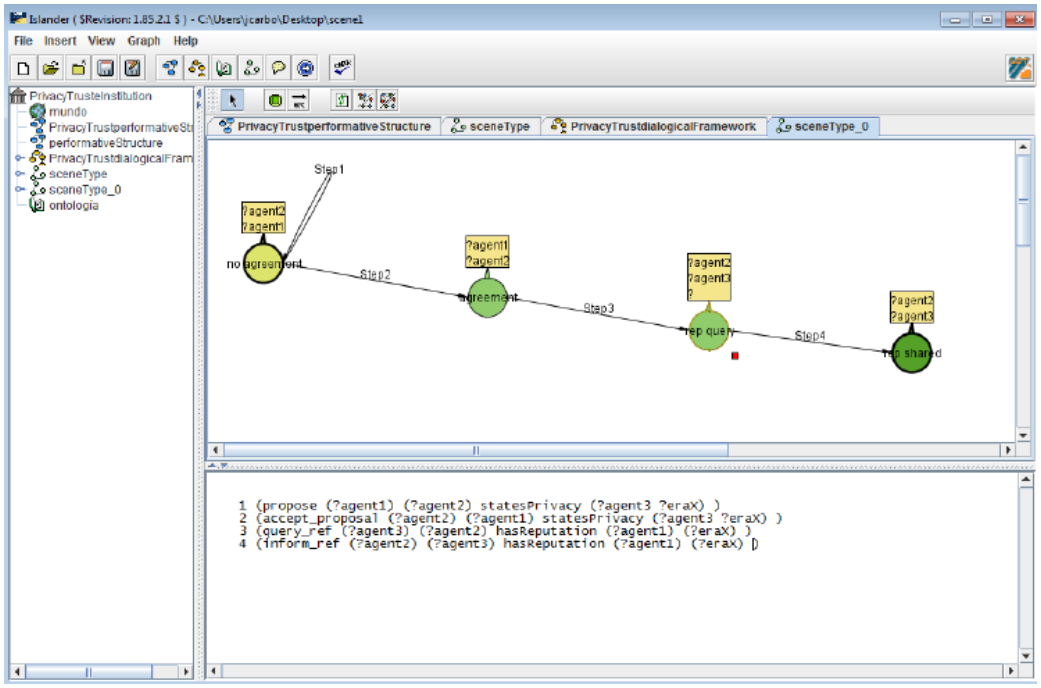

Figura 6.11. Captura de pantalla Islander, Scene 2

3. Scene 3: El “Agent1” pregunta al “Agent2” si está adquiriendo información sobre su reputación, y el “Agent2” informa que no lo está haciendo; si bien el “Agent1” también está solicitando esta información al “Agent3” (step 3). El agente pasa por los estados “query collect”, “inform no collect”, “query reputation” y “shared reputation”.

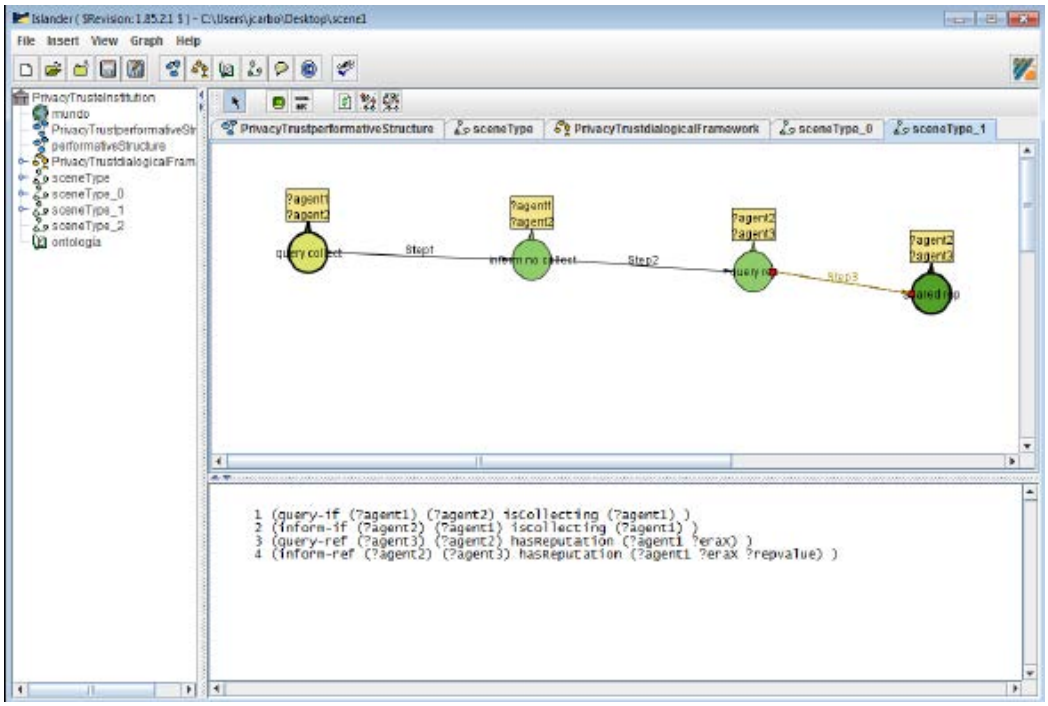

Figura 6.12. Captura de pantalla Islander, Scene 3

4. Scene 4: El “Agent1” pide al “Agent2” que bloquee o elimine la información sobre su reputación (step 1), y el “Agent2” declara que la acción de eliminación se ha realizado (step 2); si bien el “Agent2” está realizando peticiones de información al “Agent3” sobre el “Agent1” (steps 3-4). El agente pasa por los estados “request blocking”, “done blocking”, “query reputation”, “inform reputation” y “shared reputation”.

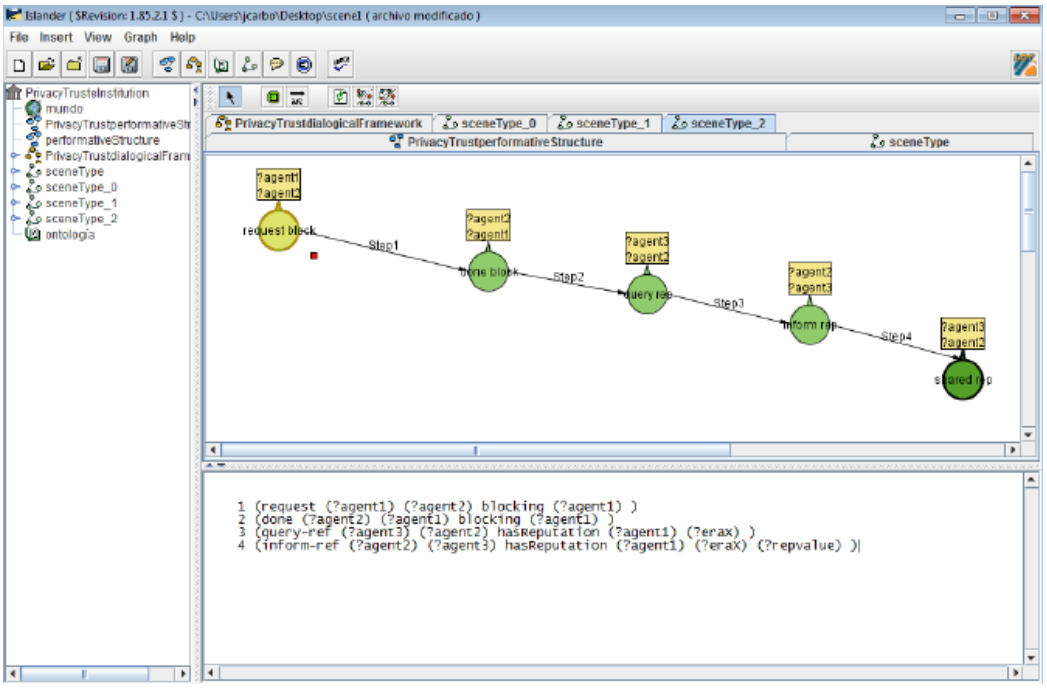

Figura 6.13. Captura de pantalla Islander, Scene 4

5. Scene 5: el “Agent1” solicita al “Agent2” la justificación de la información de su reputación (step 1), el “Agent2” contesta a la pregunta (step 2), pero el “Agent1” no está satisfecho con la justificación que le ofrece el “Agent2”, y entonces le solicita que rectifique con otra evaluación sobre su reputación (step 3). El “Agent2” confirma que esta acción de rectificación ha sido realizada (step 4), mientras que responde a las peticiones del “Agent3” sobre el “Agent1” sin rectificar la evaluación de su reputación (steps 5-6). El Agente pasa por los estados “query justification”, “inform justification”, request rectifying”, “done rectifying”, “query reputation”, “inform reputation” y “shared reputation”.

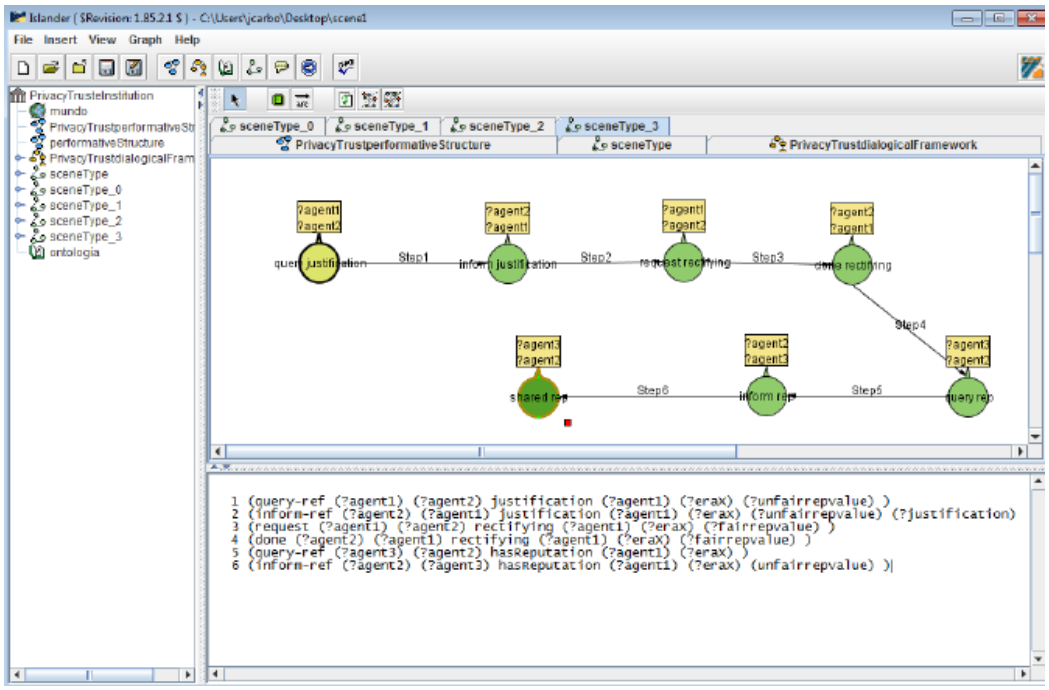

Figura 6.14. Captura de pantalla Islander, Scene 5

En estos cinco escenarios, el “Agent1” actúa como agente cuya privacidad ha sido vulnerada, el “Agent2” actúa como agente infractor de la privacidad, y el “Agent3” actúa como un tercero que se encuentra involucrado en la infracción de la privacidad.

Adicionalmente, se han definido para cada uno de los agentes, dos acciones que se ejecutan de forma alternativa:

- Acciones reversibles de forma voluntaria del agente infractor de la privacidad, guardando el daño causado sobre la información acerca de la reputación del “Agent1”.

- Obligaciones forzosas que tiene que cumplir el agente infractor de la privacidad (o de los agentes que le representan), establecidas por la Institución Electrónica para mantener la privacidad del “Agent1”.

Estas acciones tienen lugar en los cinco escenarios de privacidad definidos:

- En la Scene 1, el "Agent2" se había olvidado de informar al "Agent1". Esta situación representa el menor daño de privacidad posible. El "Agent2" puede enviar solamente el mensaje informativo al "Agent1" (step 1), solicitando la recogida de su información (step 2). Es decir, la Institución Electrónica (o algún otro agente actuando en su nombre con un papel sancionador), informaría al "Agent1" sobre las intenciones de adquirir información del "Agente2".

- En las Scene 2 y 3, el "Agent2 ha engañado de manera consciente al "Agent1". En esta situación, el "Agent2" puede informar voluntariamente al "Agent3" del hecho de no estar autorizado para compartir la información sobre la reputación del "Agent1", y también puede informar junto con el "Agent1", diciendo que el "Agent3" tiene esta información sobre él, y que podría no haber sido adquirida directamente por él (de esta forma, el "Agent1" puede solicitar después al "Agente3", la retirada de esta información). Es decir, la Institución Electrónica (o algún agente actuando en su nombre con un papel sancionador) informaría directamente al "Agent1" y al "Agent3" sobre esta circunstancia.

- En la Scene 4, el "Agent2" ha engañado de manera consciente al "Agent1". En esta situación, el "Agent2" puede retirar de forma voluntaria la información sobre la reputación del "Agent1" (solicitada mediante la eliminación o bloqueo), y también puede informar junto con el "Agent1", diciendo que el "Agent3" tiene esta información sobre él, y que podría no haber sido adquirida por ninguno (de esta forma, el "Agent1" puede solicitar después al "Agent3", la retirada de esta información). Es decir, la Institución Electrónica (o algún agente actuando en su nombre con un papel sancionador), informaría directamente al "Agent1" y al "Agent3" sobre esta circunstancia. En este caso, como la Institución Electrónica no tiene evidencias de que la información sobre la reputación del "Agent1" haya sido retirada, enviaría un mensaje informando a todos los agentes del sistema diciendo que el "Agent2" no está autorizado a compartir dicha información sobre el "Agent1".

- En Scene 5, el “Agent2” ha engañado de manera consciente al “Agent1”. En esta situación, el “Agent2” puede rectificar voluntariamente la evaluación de la reputación sobre el “Agent1” (que ha sido solicitada), y también puede informar junto con el “Agent1” sobre la rectificación de la evaluación de la reputación al “Agent3”. Es decir, la Institución Electrónica (o algún agente actuando en su nombre con un papel sancionador), informaría directamente al “Agent3” sobre la evaluación real final de la reputación del “Agent1”. En este caso, la Institución Electrónica con el fin de evitar la difusión de la mala reputación sobre el “Agent1”, informaría a todos los agentes del sistema que el “Agent2” no dispone de información rigurosa (fiable) sobre la reputación del “Agent1”.

6.6. CONCLUSIONES

Utilizando el concepto “Privacy by Design” hemos establecido las diferentes políticas de privacidad para presentar el modelo conceptual de privacidad en Inteligencia Ambiental, que nos han permitido establecer el nivel de protección de la información requerido, según el dominio de aplicación del AmI en el que se encuentra el usuario. A partir de este modelo conceptual, se ha determinado cómo deben ser las comunicaciones en los agentes de los modelos de confianza, para definir el Modelo de Privacidad Digital en AmI basado en Sistemas Multiagente, este sistema nos permitirá definir las condiciones legales de protección de la privacidad de nuestra información personal que debe cumplir nuestro modelo de confianza.

A partir de las políticas de privacidad que hemos establecido y que deben cumplir los agentes de nuestro modelo de confianza en sus comunicaciones, se han definido los seis derechos de privacidad que deben ser cumplidos por los agentes involucrados en nuestro modelo.

La integración de estos seis derechos de privacidad en las comunicaciones entre los agentes de nuestro modelo de confianza, han sido incluidas mediante el intercambio de mensajes adicionales, éstos podrían actuar como mecanismos de control permitiendo, así, a los agentes del modelo de confianza, satisfacer estos derechos. Estos mensajes adicionales han sido formalizados mediante protocolos que deben ser intercambiados entre nuestros agentes, protegiéndose de esta manera la privacidad en sus comunicaciones.

El Modelo de Privacidad Digital en AmI basado en Sistemas Multiagente propuesto, ha sido implementado para su validación en el dominio del ART (Agent Reputation and Trust), que nos ha servido para definir los cinco protocolos o mensajes de comunicación adicionales entre los agentes, y dar así cumplimiento a los seis derechos de privacidad que hemos establecido (en conformidad con FIPA). Estos mensajes implementados en JADE, incluyen los correspondientes conceptos, predicados y acciones, necesarios para definir el contenido de estos mensajes. A continuación hemos utilizado WEKA como herramienta de aprendizaje automático, para llevar a cabo la tarea de decidir con qué agente compartimos nuestras opiniones privadas, que será el que el modelo nos muestre como agente fiable.

Para terminar, hemos considerado conveniente verificar el cumplimiento legal de los derechos de privacidad establecidos, por lo que hemos formalizado las restricciones o infracciones de privacidad que pueden darse en la transmisión de la información entre los agentes, para lo cual se ha utilizado la Institución Electrónica “Islander”.

PARTE IV

CONCLUSIONES

Y TRABAJO FUTURO

Capítulo 7

Conclusiones y Trabajo Futuro

7.1. DISCUSIÓN Y CONCLUSIONES

La Inteligencia Ambiental engloba una amplia variedad de dispositivos y tecnologías con capacidades de computación y comunicación, destinada a ofrecernos multitud de servicios en cualquier lugar y en todo momento, facilitándonos así la realización de la mayoría de nuestras actividades cotidianas.

Son indiscutibles los beneficios que nos ofrecen los entornos inteligentes desarrollados en Inteligencia Ambiental, pero, también suponen un riesgo para la protección de nuestra información personal, teniendo en cuenta la gran cantidad de información de distinta naturaleza que los diferentes dispositivos y tecnologías presentes en estos entornos son capaces de adquirir, almacenar, compartir y transmitir, viéndose de esta forma comprometida nuestra protección de la privacidad.

Uno de los principales objetivos en el desarrollo de los entornos inteligentes del AmI, es que las tecnologías presentes en los mismos sean invisibles para el usuario, pensándose que de esta forma resultan más útiles para él, pero, teniendo en cuenta los riesgos que suponen para la protección de nuestra información privada, consideramos que la forma en la que debe mostrarse al usuario es siendo transparente.

Teniendo en cuenta que, el objetivo final de la Inteligencia Ambiental es el de facilitar y mejorar la vida de las personas a través de los servicios personalizados ofrecidos y, considerando los principales aspectos, tanto técnicos como sociales que deben integrarse en los sistemas del AmI, se han establecido los componentes socio-tecnológicos que fundamentan las aplicaciones desarrolladas en Inteligencia Ambiental (Figura 1.2.).

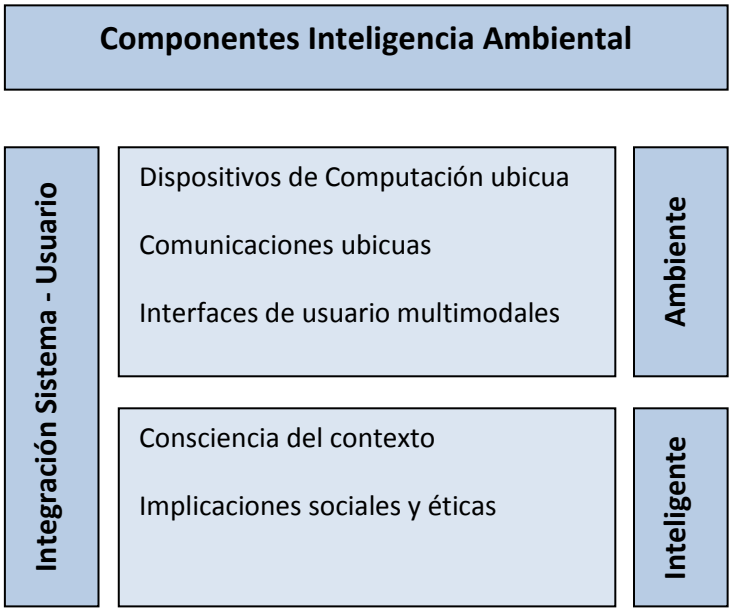

Figura 1.2. Componentes socio-tecnológicos del AmI

Atendiendo a estos fundamentos, y considerando el hecho de que el centro de atención de las aplicaciones del AmI es el usuario, creemos necesario que en el desarrollo de las aplicaciones de la Inteligencia Ambiental no solo hay que tener en cuenta los aspectos tecnológicos (derivados del uso de los dispositivos de comunicación y computación), sino que, deben incluirse como base de su diseño las cuestiones relacionadas con los aspectos sociales y éticos, entre las que hemos destacado la privacidad, por ser uno de los derechos fundamentales de las personas como así queda reflejado en la Declaración Universal de los Derechos Humanos (Artículo 12) y en otras disposiciones legales (Convención Europea de los Derechos Humanos (Artículo 8), Acta Europea de los Derechos Humanos (Artículos 7 y 8), y en nuestra Constitución Española de 1978 (Artículo 18)).

Así pues, y con el objetivo de proteger la privacidad de nuestra información personal al acceder a los servicios ofrecidos por la Inteligencia Ambiental, hemos considerado que sean las propias técnicas utilizadas en las aplicaciones del AmI las que nos ayuden a preservarla. Por ello, se ha realizado un estudio de las mismas, que ha permitido establecer una clasificación de las aplicaciones del AmI atendiendo a los dominios de aplicación del AmI y a las tecnologías utilizadas (Figura 3.2.).

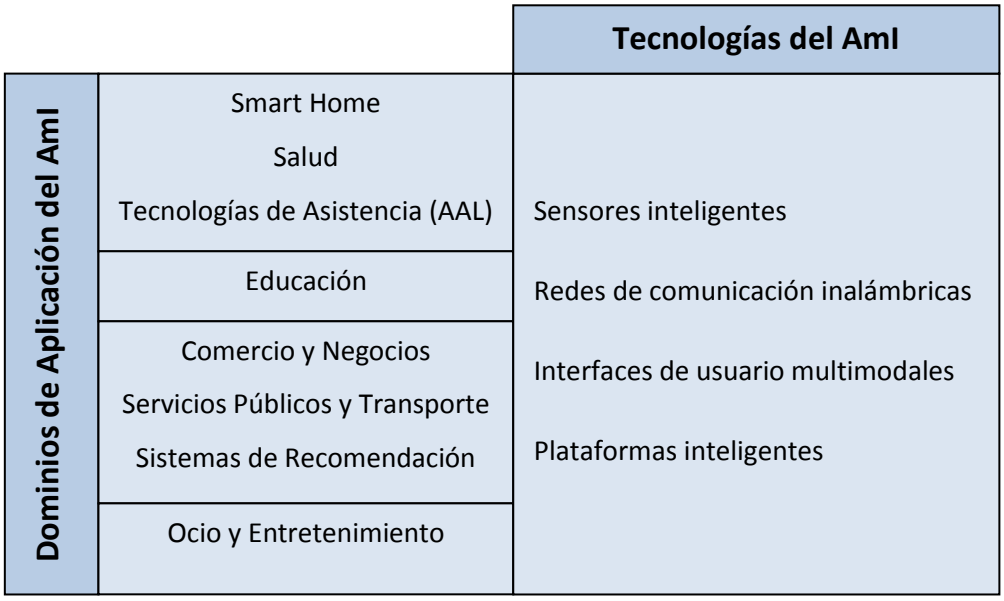

Figura 3.2. Dominios y Tecnologías de las Aplicaciones del AmI

De la revisión realizada de las aplicaciones desarrolladas en Inteligencia Ambiental se concluye que, la mayoría de ellas se encuentran dirigidas al desarrollo e integración de las tecnologías utilizadas (dispositivos computacionales y dispositivos de comunicación), en algunos casos se encuentran focalizadas en la usabilidad por parte del usuario y, en muy pocos casos tienen en cuenta las cuestiones sociales y el impacto de la privacidad que supone el uso de las mismas. Además, el estudio ha constatado la gran cantidad de información personal que puede ser adquirida, almacenada, gestionada y transmitida, por los dispositivos y tecnologías presentes en los dominios de aplicación del AmI, lo que conlleva a elevar los riesgos relativos a la protección de la privacidad de los usuarios.

A partir de este estudio se han determinado los aspectos tecnológicos y sociales más relevantes que deben ser considerados para el verdadero desarrollo y aceptación de la Inteligencia Ambiental (Figura 3.21.). Considerando estos aspectos socio-tecnológicos y teniendo en cuenta que los servicios desarrollados en las aplicaciones del AmI deben cubrir las necesidades de los usuarios, aumentando de esta forma su grado de aceptación y confianza, el trabajo de investigación se centró en la protección de la privacidad que deben ofrecernos dichas aplicaciones.

Aplicaciones del AmI			
Aspectos tecnológicos	Automatización Eficiencia energética Nanotecnología Usabilidad Aprendizaje Monitorización Comunicación	Protección Asistencia Confort Seguridad Confianza Privacidad Conocimiento	Aspectos sociales

Figura 3.21. Aspectos socio-tecnológicos de las aplicaciones del AmI

A continuación se presentó el marco legal del derecho a la privacidad, que sirvió para determinar las distintas disposiciones legales tanto a nivel nacional como europeo que lo regulan, poniendo de manifiesto el complejo marco legal en el que se encuentra inmerso el derecho a la privacidad, con distintas normas sobre los dispositivos y tecnologías de computación y comunicación.

En base a estas consideraciones, la investigación se centró en los estudios realizados sobre la privacidad en Inteligencia Ambiental. La mayoría de los trabajos realizados se encuentran focalizados principalmente en los mecanismos de obtención y control de la información adquirida y procesada, y no tienen en cuenta la naturaleza de los sistemas desarrollados en AmI que son distribuidos y dinámicos. Otros de los estudios tratan de cuantificar la privacidad mediante la utilización de diferentes tipos de medidas. Los estudios realizados sobre la privacidad en AmI en la última década, han ido dirigidos a presentar los modelos de recomendación y confianza como una de las estrategias más útiles para la protección de nuestra privacidad.

Teniendo en cuenta que la divulgación de nuestra información sin nuestro consentimiento y conocimiento significa la pérdida de nuestra privacidad, la confianza en la transmisión de la misma, puede servir para minimizar los riesgos de privacidad de nuestra información. Esta ha sido la hipótesis planteada en este trabajo de investigación, la utilización de los agentes en los modelos de confianza como herramienta para minimizar los riesgos de privacidad de nuestra información personal.

Así pues, el objetivo de esta tesis ha sido el de presentar un Modelo de Privacidad Digital basado en Sistemas Multiagente que nos ayude a decidir en quién confiamos a la hora de compartir nuestras opiniones privadas, minimizando así los riesgos de privacidad de nuestra información. Para alcanzar este fin, se ha llevado a cabo la realización de diferentes objetivos específicos que se describen a continuación.

En primer lugar, se ha realizado un estudio sobre las aplicaciones desarrolladas en Inteligencia Ambiental, que ha permitido establecer una clasificación de las mismas, atendiendo al dominio de aplicación del usuario y a las tecnologías utilizadas en los mismos.

Atendiendo a esta clasificación se ha definido el marco conceptual de privacidad en AmI “Design by Privacy” (Figura 5.2.) que establece las diferentes políticas de privacidad que deben ser consideradas en el diseño de las aplicaciones desarrolladas en AmI para preservar la privacidad de la información. Estas políticas de privacidad han servido para evaluar el grado de protección requerido de la información personal de los usuarios, según el dominio de aplicación en el que se encuentren.

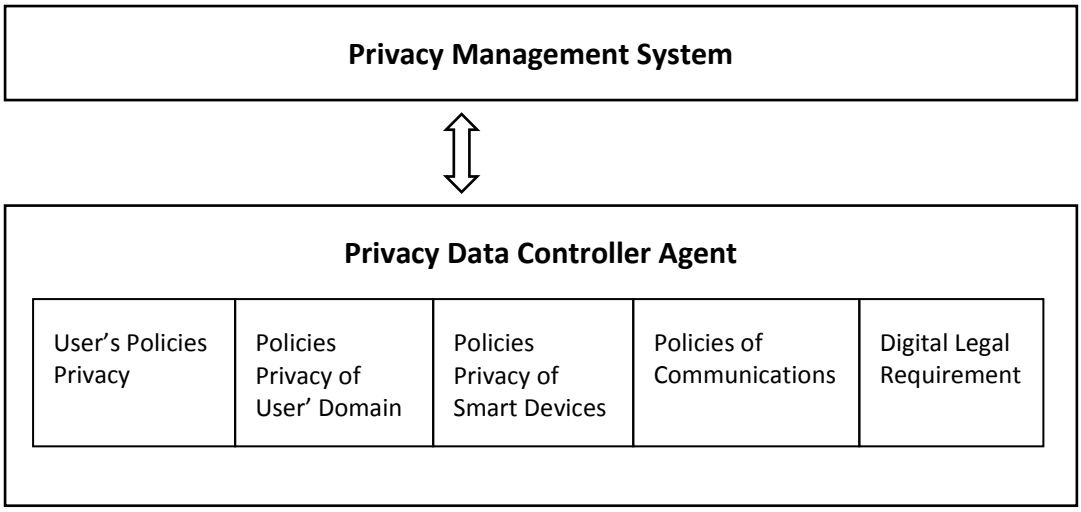

Figura 5.2. Modelo conceptual "Design by Privacy" en Inteligencia Ambiental

A partir de las políticas de privacidad establecidas en el modelo conceptual "Design by Privacy", y teniendo en cuenta los diferentes niveles de protección de la información (cumpliendo con la normativa legal que regula la protección de los datos en la Unión Europea, Regulation EU, 2016/679), se han determinado los derechos de privacidad que deben cumplir los agentes de nuestro modelo de confianza en sus comunicaciones.

La integración de estos derechos de privacidad en nuestro modelo de agentes de confianza se ha llevado a cabo con la propuesta de una serie de mensajes adicionales que deben cumplir los agentes en los protocolos de las relaciones de confianza del entorno de experimentación ART testbed (Agent Reputation and Trust), en el que el dominio de aplicación del AmI es el relacionado con la tasación de cuadros o pinturas de arte. De esta forma, es como se ha establecido la protección de la privacidad de la comunicación entre los agentes de nuestro modelo de confianza (Figura 6.3.).

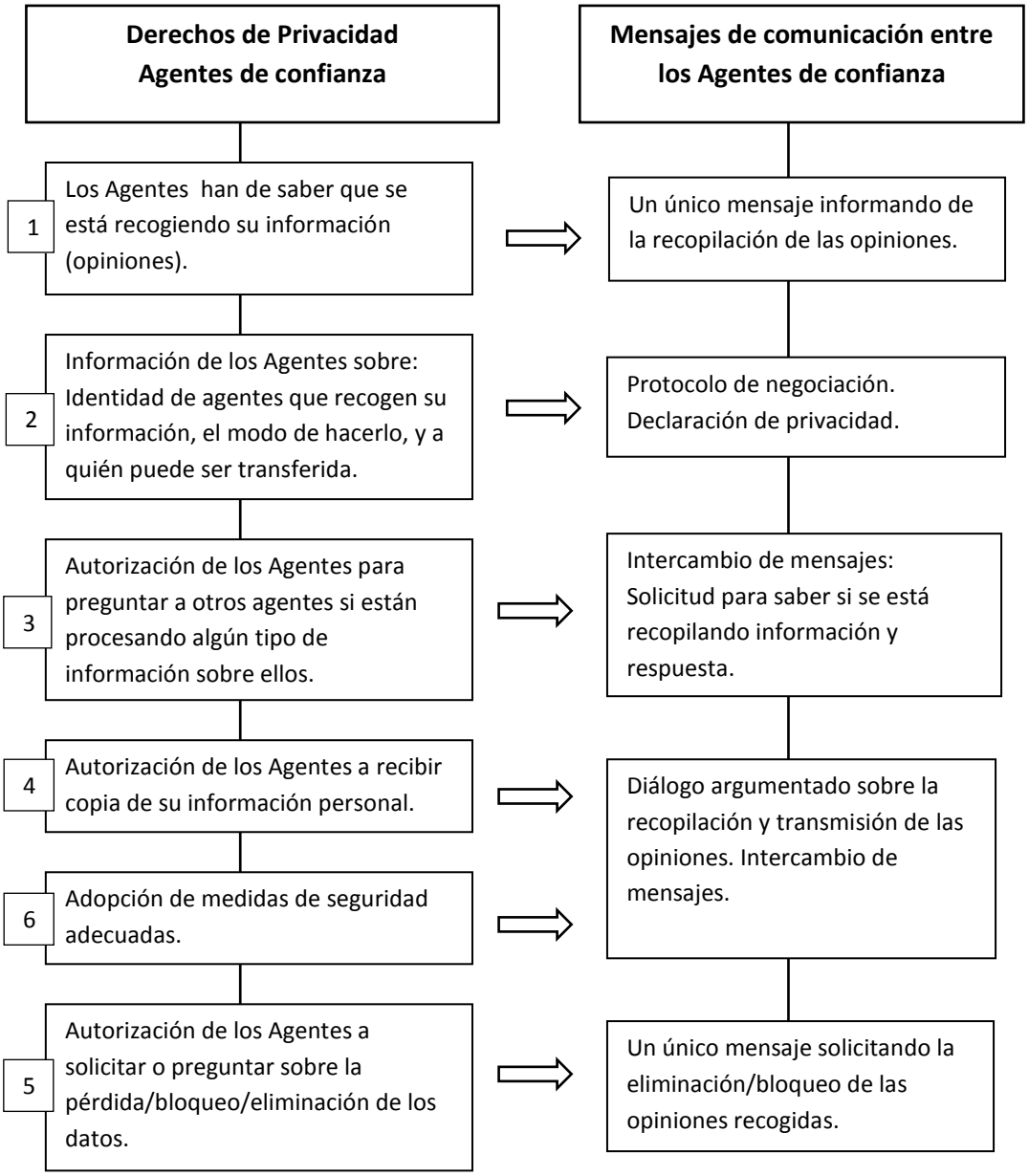

Figura 6.3. Protección de la Privacidad de la Comunicación entre los Agentes de confianza

La implementación de los mensajes adicionales en la comunicación entre los agentes de confianza que dan cumplimiento con los derechos de privacidad establecidos, ha sido realizada en el entorno de experimentación del ART testbed.

Para ello, se han formalizado siguiendo el estándar FIPA (Foundation for Intelligent Physical Agents) los protocolos de comunicación utilizando la plataforma del ART testbed implementada en el entorno de JADE (Figura 6.4.). Estos mensajes incluyen los correspondientes conceptos, predicados y acciones necesarios que definen el contenido de los mensajes intercambiados entre los agentes de nuestro modelo de privacidad digital dando, así, cumplimiento a los derechos de privacidad establecidos.

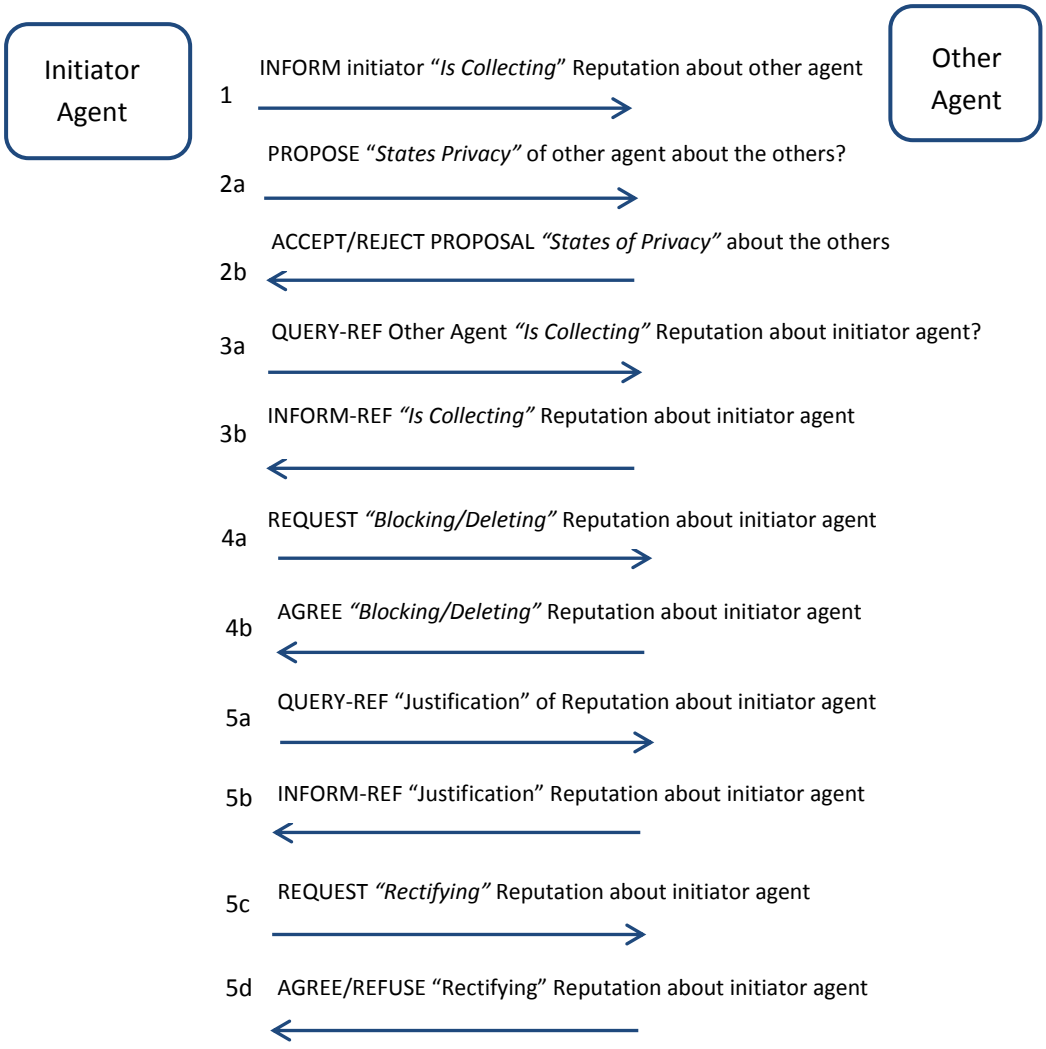

Figura 6.4. Protocolos de protección de la Privacidad en JADE en el dominio del ART

Una vez implementado el modelo de privacidad digital que da cumplimiento a los derechos de privacidad establecidos en las comunicaciones entre los agentes involucrados, se valida la propuesta utilizando los datos de la competición del ART testbed de 2007, en la que se comparan las opiniones de tres agentes sobre una colección de 57 cuadros con la estimación final de los mismos. Para ello, se define la manera en la que vamos a decidir quiénes son los agentes merecedores de compartir con ellos nuestras opiniones privadas (decisión binaria), utilizando WEKA como herramienta de aprendizaje automático.

Se han establecido unos atributos de entrada (valores de las opiniones de nuestros agentes) y un atributo como salida (nuestra variable objetivo a predecir, CLASE), para determinar cuáles son los agentes en los que vamos a confiar para compartir nuestras opiniones privadas (Figura 6.5.), que serán los agentes cuyo valor se aproxime más al valor real de estimación final, y que definirá el objetivo CLASE.

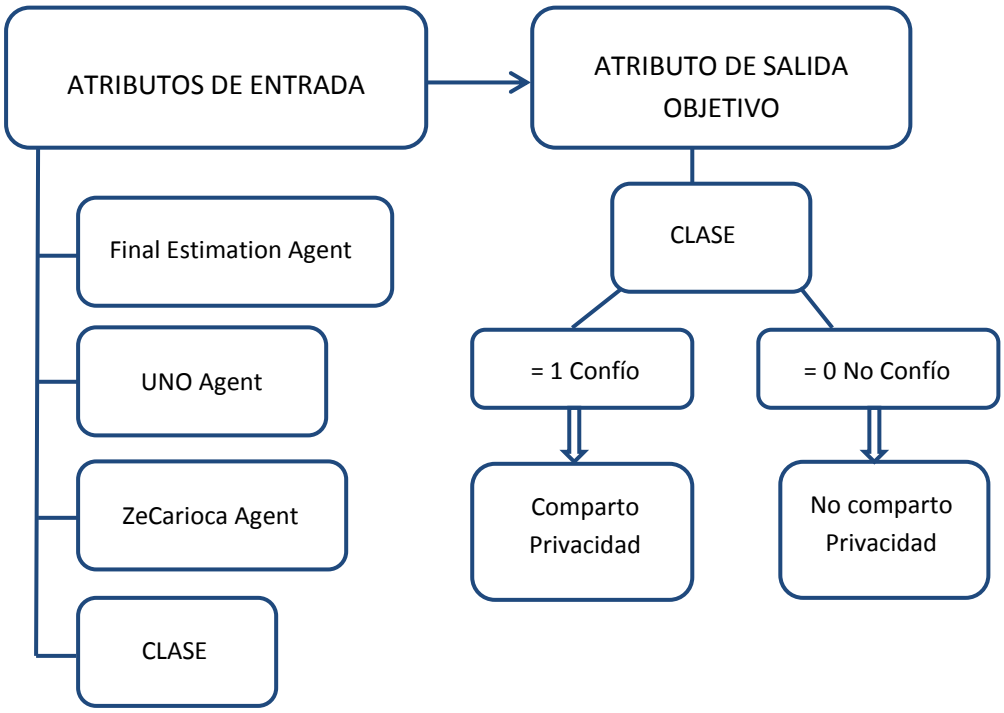

Figura 6.5. Atributos del modelo de privacidad digital en WEKA

El método de evaluación del clasificador utilizado para poder comparar nuestra CLASE objetivo fue el Cross-Validation, ya que fue con el que mayor número de aciertos se obtuvo. Una vez elegido el método de evaluación del clasificador, se prepararon tres tipos de escenarios con diferentes opiniones sobre los cuadros (Figura 6.6.) a los que se aplicaron diferentes algoritmos de clasificación (MLP, J48, RBF Network, PART, RIDOR, OneR, TreesLMT). De esta forma, se obtuvo el número de instancias clasificadas correctamente de acuerdo a nuestra CLASE objetivo (Figura 6.7.).

Setting 1 = Window size 4 (57 rows, 228 instances)

Setting 2 = Window size 7 (56 rows, 392 instances)

Setting 3 = Window size 10 (54 rows, 540 instances)

Figura 6.6. Tipos de escenarios propuestos para compartir nuestras opiniones privadas

CLASE = 1 → Confío → Comparto Privacidad

CLASE = 0 → No Confío → No comparto Privacidad

Figura 6.7. Decisión final para compartir nuestras opiniones privadas

Los resultados obtenidos muestran el porcentaje de aciertos por clasificador teniendo en cuenta los tres escenarios establecidos (Tabla 6.1.), estando la mayoría de ellos comprendidos entre el 55-65% de aciertos. Estos valores de aciertos representan la decisión de confiar o no en un agente por lo que, considerando que los valores más altos se encuentran entre el 68,42-70,17% significa que aproximadamente un 30% de las evaluaciones realizadas no nos ayudan a decidir si confiamos o no en el agente para compartir nuestras opiniones privadas.

Classifier	Window size 4	Window size 7	Window size 10
MLP	70,175	55,357	60,377
J48	54,386	64,285	56,603
RBF Network	68,421	58,928	49,056
PART	54,386	58,928	50,943
RIDOR	56,140	62,500	56,603
OneR	61,403	58,928	54,717
TreesLMT	61,403	55,357	52,830

Tabla 6.1. Valores del porcentaje de aciertos por clasificador en los tres tipos de escenarios

Después de haber validado la manera de decidir con quién compartimos nuestra información privada, y con el fin de controlar el cumplimiento de los derechos de privacidad establecidos, se ha considerado conveniente definir las posibles infracciones de privacidad que pueden tener lugar en las comunicaciones entre los agentes. Estas infracciones de privacidad han sido expresadas de la siguiente forma:

1. Un “1st/2nd Agent” adquiere las opiniones sobre otro agente, sin su conocimiento (no se ha enviado ningún mensaje previo informando de esta acción).

2. Un “2nd Agent” envía las opiniones sobre un “3rd Agent” al “1st Agent”, las cuales no estaban incluidas en la correspondiente declaración de privacidad del “3rd Agent”.

3. Un “2nd Agent” que ha sido informado con opiniones incompletas o incorrectas sobre un 3rd Agent”, envía una serie de opiniones diferentes o más ampliadas sobre él al “1st Agent”.

4. Un “1st/2nd Agent” que ignora la orden de bloquear o eliminar las opiniones adquiridas, y sigue transmitiendo dicha información.

5. Un “1st/2nd Agent” que no explica el motivo por el que las opiniones sobre un “3rd Agent” están siendo difundidas, es decir, no responde a la petición de justificación del “3rd Agent”.

6. Posibilidad de que los agentes rompan la seguridad de las comunicaciones donde las opiniones han sido difundidas: un “1st Agent” transmitiendo las opiniones sobre un “3rd Agent”, sin que la adquisición de las mismas haya sido realizada con una aprobación previa (directa o indirectamente) por parte de ningún “2nd/3rd Agent”.

Para terminar, estas infracciones han sido formalizadas a través de la Institución Electrónica “Islander”, utilizada como herramienta de especificación de las normas y sanciones correspondientes que deben cumplir los agentes en sus comunicaciones, a través de la representación gráfica de cinco escenas que representan las interacciones que tienen lugar entre los agentes participantes (Agent1, agente cuya privacidad ha sido vulnerada; Agent2, agente infractor de la privacidad; Agent3, agente involucrado en la infracción de la privacidad). Además en cada una de las escenas representadas se han definido dos acciones adicionales para cada uno de los agentes que se ejecutan de forma alternativa: acciones reversibles de forma voluntaria del agente infractor de la privacidad, y obligaciones forzosas que debe cumplir el agente infractor de la privacidad.

7.2. Trabajos Futuros

El trabajo de investigación presentado supone un pequeño paso hacia el verdadero establecimiento de políticas de privacidad en el diseño de las aplicaciones desarrolladas en Inteligencia Ambiental, por lo que debe seguir trabajándose en la implementación y desarrollo del marco conceptual de privacidad en AmI presentado "Design by Privacy".

A partir de esta idea, surgen nuevos retos relacionados con el diseño e implementación de las medidas de protección de los distintos niveles de privacidad establecidos en el Sistema de Gestión de la Privacidad en otros dominios de aplicación del AmI (acceso a los datos/responsabilidades/localización de los datos/distribución de los datos/recuperación de los datos/soporte técnico de actividades ilegales). Otra posible línea de investigación es la forma de fusionar las políticas de privacidad de los diferentes módulos que componen el Agente Controlador de Privacidad.

También resulta de interés implementar y validar el Modelo de Privacidad Digital en AmI basado en Sistemas Multiagente en el dominio del Ambient Assisted Living (AAL), por tratarse de un dominio en el que el colectivo de usuarios que interaccionan con los servicios ofrecidos por el AmI es especialmente vulnerable.

Otras futuras líneas de investigación pueden ir dirigidas al establecimiento de controles técnicos que aseguren la protección de la privacidad en un determinado dominio del AmI. Así, como las dirigidas a la identificación de las amenazas reales de los usuarios teniendo en cuenta el dominio de aplicación del AmI en el que se encuentran y/o considerando la naturaleza de la tecnología presente.

Un gran reto como línea de investigación sería el diseño de aplicaciones en Inteligencia Ambiental dirigidas a ayudar a colectivos especiales como puede ser el de las víctimas de la violencia de género, y el de los menores de edad; ofreciéndoles herramientas que les ayuden a preservar su derecho a la privacidad.

7.3. PUBLICACIONES RELACIONADAS

Durante el desarrollo de esta tesis se han publicado varios artículos en revistas internacionales, capítulos de libro, así como, varias aportaciones a congresos, workshops y conferencias.

7.3.1. Publicaciones en Revistas Internacionales

- Mar López, Javier Carbó, José M. Molina, Juanita Pedraza. Electronic institutions and neural computing providing law-compliance privacy for trusting agents. Publishing in the Journal of Applied Logic JAL-450, 2016. http://dx.doi.org/10.1016/j.jal.2016.11.019. (November 2016). Incluida en la Science Edition del ISI-JCR, área de IA y ciencias de la computación.

- Mar López, Juanita Pedraza, Javier Carbó, José M. Molina. The awareness of Privacy issues in Ambient Intelligence. Publishing in the Advances in Distributed Computing and Artificial Intelligence Journal, ADCAIJ-2014, Volume 3, number 2, (September 2014).

7.3.2. Publicaciones en Capítulos de Libro

- Mar López, Juanita Pedraza. Chapter Privacy Risks in Cloud Computing in the Book Intelligent Agents in Data intensive Computing. Publishing in Studies in Big Data Series, Volume 14, pp. 163-192 (2016).

7.3.3. Publicaciones en Congresos, Workshops, Conferencias

- Mar López, Javier Carbó, José M. Molina. Costs of Protecting Privacy in Agent Trust Relationships. PAAMS-2015, Workshop on Highlights of Practical Applications of Agents and Multi-Agent Systems and Sustainability (June 2015 Salamanca, Spain). Publishing in the CCIS series, Communications in Computer and Information Science series, Volume 524, pp. 179-190. (April 2015).

- Javier Carbó, Juanita Pedraza, Mar López, José M. Molina. Privacy Protection in Trust Models for Agent Societies. SOCO-2014, International Joint Conference SOCO´14-CISIS´14-ICEUTE´14 (June 2014 Bilbao, Spain). Proceedings of the Advances in Intelligent Systems and Computing, Volume 299, pp. 135-144, (2014).

- Mar López, Juanita Pedraza, Javier Carbó, José M. Molina. Ambient Intelligence: Applications and Privacy Policies. PAAMS-2014, Workshop on Intelligent Systems for Context-based Information Fusion (June 2014 Salamanca, Spain). Publishing in the CCIS series, Communications in Computer and Information Science series, Volume 430, pp. 191-201, (April 2014).

- Javier Carbó, Juanita Pedraza, Mar López, José M. Molina. An Approach to Privacy Protection in Trust Models for Agent Societies. ACySE-2014, Workshop AAMAS International Conference on Autonomous Agents and Multiagent Systems (March 2014 Paris, France).

7.4. PROYECTOS RELACIONADOS

En el transcurso de los años dedicados a la investigación de esta tesis he tenido la oportunidad de colaborar con distintas entidades públicas y privadas a través de diferentes proyectos de I+D+I.

7.4.1. Participación en Proyectos I+D+i financiados en convocatorias públicas

- Proyecto TEASE: Técnicas de Estimación de Actividad para Servicios en Espacios Inteligentes (Año Inicio: Enero 2013–Año Fin: Junio 2016). Proyecto Coordinado de Investigación Nacional. Universidad Carlos III de Madrid. Investigador Principal y Coordinador: José Manuel Molina. Entidad que subvenciona: Ministerio de Ciencia e Innovación. Entidades participantes: Universidad Politécnica de Madrid, Universidad Carlos III de Madrid.

- Proyecto CONTEXTS: Conceptos y Tecnologías para el Desarrollo de Servicios Contextuales (Año Inicio: Enero 2010–Año Fin: Mayo 2014). Proyecto Coordinado de Investigación Nacional. Universidad Carlos III de Madrid. Investigador Principal: José Manuel Molina. Coordinador: José Ramón Casar Corredera. Entidad que subvenciona: Comunidad de Madrid. Entidades participantes: Universidad Politécnica de Madrid, Universidad Alcalá de Henares, Universidad Autónoma de Madrid, Universidad Carlos III de Madrid.

- Proyecto INFUSA: Integración de Técnicas de Fusión e Interpretación para el Desarrollo de Servicios basados en Estimación de Actividad en Espacios Inteligentes (Año Inicio: Enero 2012–Año Fin: Diciembre 2012). Proyecto Coordinado de Investigación Nacional. Universidad Carlos III de Madrid. Investigador Principal y Coordinador: José Manuel Molina. Entidad que subvenciona: Ministerio de Ciencia e Innovación. Entidades participantes: Universidad Politécnica de Madrid, Universidad Carlos III de Madrid.

- Proyecto MADRINET: Multidisciplinary Advanced Research in User-Centric Wireless Network enabling Technologies (Año Inicio: Enero 2006–Año Fin: Diciembre 2009). Proyecto Coordinado de Investigación Regional. Universidad Carlos III de Madrid. Investigador Principal: José Manuel Molina. Coordinador: José Ramón Casar Corredera. Entidad que subvenciona: Comunidad de Madrid. Entidades participantes: Universidad Politécnica de Madrid, Universidad Alcalá de Henares, Universidad Carlos III de Madrid.

7.4.2. Participación en Proyectos I+D+i financiados con entidades privadas

- Proyecto: e-TUR2020 Turismo & Retail (Año Inicio: Julio 2015–Año Fin: Julio 2019). Proyecto privado. Universidad Carlos III de Madrid. Investigador Principal: Miguel Ángel Patricio. Entidad que subvenciona: SOLUSOFT.

- Proyecto: Asesoramiento y asistencia técnica en el área de análisis de los riesgos tecnológicos que se establecen en el acceso a la información y la privacidad de la misma (Boss in the Box) (Año Inicio: Marzo 2013–Año Fin: Octubre 2014). Proyecto privado. Universidad Carlos III de Madrid. Investigador Principal: José Manuel Molina. Entidad que subvenciona: SOITSA.

- Proyecto: Diseño e Implementación del Proceso de Fusión de Datos del programa SIGINT (Año Inicio: Febrero 2011–Año Fin: Enero 2013). Proyecto privado. Universidad Carlos III de Madrid. Investigador Principal: José Manuel Molina. Entidad que subvenciona: AIRBUS.

[Eli Zelkha and Epstein B., 1998]. From Devices to 'Ambient Intelligence'. Digital Living Room Conference, 1998.

[ISTAG, 2001]. Scenarios for ambient intelligence in 2010. European Commission report.http://www.cordis.lu/ist/istag.html, 2010.

[ISTAG, 2002]. Strategic orientation & priorities for IST in FP6. European Commission Report, http://www.cordis.europa.eu/fp/ict/istag/reports_en.html, 2010.

[7PM] https://ec.europa.eu/research/fp7/understanding/fp7inbrief/what-is_es.html, 2012.

[ISTAG, 2003]. Ambient Intelligence: from vision to reality, European Commission Report, http://www.cordis. europa.eu/fp7/ict/istag/reports_en.html,2010.

[H2020] http://ec.europa.eu/programmes/horizon2020/, 2017.

[E.H.L. Aarts et al. 2001]. Ambient Intelligence, in: J. Denning (ed.) The Invisible Future, MacGraw Hill, New York, NY, USA, pp. 235-251, 2001.

[M. Weiser, 1991-1992]. The Computer for the Twenty-First Century, Scientific Am 162(3), 94-104, 1991-92.

[Gaggioli, A. 2005]. Optimal experience in ambient intelligence. In Ambient Intelligence, G. Riva, F. Vatalaro, F. Davide, and M. Alcaniz, Eds., IOS Press, Amsterdam, 35-43, 2005.

[Schmidt, 2005]. Interactive context-aware systems. Intering with Ambient Intelligence. In Ambient Intelligence: Riva G, Vatalaro F, David F, Alcañiz M (eds): The evolution of technology, communication and cognition towards the future of human-computer interaction. IOS Press, Amsterdam, 2005.

[F. Adelstein, et al. 2004]. Fundamentals of Mobile Computing and Pervasive Computing, McGraw Hill, New York, NJ, USA, 2004.

[Punie, 2003]. A social and technological view of ambient intelligence in everyday life: What bends the trend? In: The European media and technology in everyday life network, 2000-2003. Institute for Prospective Technological Studies Directorate General Joint Research Center European Commission, 2002-03.

[Adam Greenfield, 2006]. Everyware: The Dawning Age of Ubiquitous Computing. Published March, 2006, by New Riders Publishing, 2006.

[Nava & Bravo, 2007]. Combining RFID and NFC Technologies in An AmI Conference Scenario. In Proceedings of Eighth Mexican International Conference on Current Trends in Computer Science (ENC 2007), Michoacán, México 24-28 September 2007; pp. 165-172, 2007.

[Riva, Loreti, Lungui, Vatalaro & Davide, 2003]. Presence 2010: The emergence of Ambient Intelligence. In G. Riva, F. Davide, & W. A. IJsselsteijn (Eds.), from Being there: Concepts, effects and measurement of user presence in synthetic environments. Amsterdam, The Netherlands: IOS Press, section 4, pp. 59-82, 2003.

[Reeves & Nass, 1996]. Technology and roles: A Tale of Two TVs. Journal of Communication, Vol. 46, Issue 2, pp. 121-128, 1996.

[Ferscha, A. et al. 2004]. Digital Aura. Proceedings on the 2nd International Conference on Pervasive Computing, Pervasive 2004, pp. 405-410, 2004.

[Abowd & Mynatt, 2000]. Charting past, present, and future research in ubiquitous computing. ACM Transactions on Computer-Human Interaction (TOCHI). Special issue on human-computer interaction in the new millennium, Part 1. Volume 7 Issue 1, pp. 29-58. March 2000.

[Chavira, Nava, Hervás, Bravo, & Sánchez, 2007]. Spontaneous interaction on context-aware public display: an NFC and infrared sensor approach. ImmersCom'07 Proceedings of the First International Conference on Immersive Telecommunications, Article No. 18. October 2007.

[Vincent, V.J. & Francis, K. 2006]. Interactivity of Information & Communication on large screen displays in public spaces through gestures. Proceedings on Information Visualization and Interaction Techniques for Collaboration across Multiple Displays. Workshop Associated with CHI'06. Montreal, Canada 2006.

[Dempski, K. & Harvey, B. 2006]. Multi-User Display Walls: Lessons Learned. Information Visualization and Interaction Techniques for Collaboration across Multiple Displays. Workshop associated with CHI 2006, Montreal, Canada, 2006.

[Hervás, R. et al. 2006]. Towards implicit interaction in ambient intelligence through information mosaic roles. Engineering the User Interfaces: From Research to Practice-Invited papers from Interaction springer, Heidelberg, 2006.

[Schilit, Adams & Want, 1994]. Context-Aware Computing Applications. WMCSA'94 Proceedings of the 1994 First Workshop on Mobile Computing Systems and Applications, pp. 85-90. December, 1994.

[Schilit & Theimer, 1994]. Disseminating Active Map Information to Mobile Hosts. IEEE Network. Volume 8 Issue 5, pp. 22-32, 1994.

[Ryan, Pascoe & Morse, 1997]. Enhanced Reality Fieldwork: the Context Aware Archacological Assistant. In V. Gaffney, M. v. Leusen & S. Exxon (Eds), Computer Applications in Archaelogy, 1997.

[Anind K. Dey, 2001]. Understanding and Using Context. Personal and Ubiquitous Computing. Volume 5 Issue 1, pp. 4-7 (2001).

[Karen Henricksen, Indulska, & Rakotonirainy, 2002]. Modeling Context Information in Pervasive Computing Systems. F. Mattern and M. Naghshineh (Eds), Pervasive Computing: First International Conference 2002, LNCS 2414, pp. 167-180, Zürich, 2002.

[Anind K. Dey, 2000]. Providing Architectural Support for Building Context-Aware Applications. PhD thesis, Georgia Institute of Technology, November 2000.

[Jeffrey Heer, et al. 2004]. Presiding Over Accidents: System Direction of Human Action. Proceedings of the Conference on Human Factors in Computing Systems, HCI'2004, Viena, Austria. ACM Press, 463-470, 2004.

[Anind K. Dey & J. Mankoff, 2005]. Designing Mediation for Context-aware Applications. ACM Trans. on Computer-Human Interaction. Volume 12 Issue 1, pp. 53-80, 2005.

[F. Sadri, 2011]. Ambient Intelligence: A Survey. ACM Computing Surveys, Vol. 43 Issue 4, Article 36, 2011.

[Ruyter, B. & E. Aarts, 2004]. Ambient Intelligence: Visualising the Future. Proceedings of the Advanced Visual Interfaces Conference. May, Gallipoli, Italy, pp. 203-208, 2004.

[Mark Weiser, 1993]. Hot topic: Ubiquitous computing. IEEE Computer, pp. 71-72. October 1993.

[Coen, M. 1998]. Design principles for intelligent environments. In Proceedings of the Fifteenth National Conference on Artificial Intelligence (AAAI'98), pp. 36-43. Madison, WI, 1998.

[G. Chen & Kotz, 2000]. A Survey of Context-Aware Mobile Computing Research. Technical Report TR 2000-381, Department of Computer Science, Dartmouth College, Hanover, NH. November 2000.

[http://www.songdo.com], 2016.

[Hull, R. et al. 1997]. Towards Situated Computing. In: 1st International Symposium on Wearable Computer, pp 146-153, 1997.

[Dey, AK. and Abow, GD. 1999]. Towards a Better Understanding of Context and Context-Awareness, Atlanta, Georgia: Georgia Institute of Technology, 1999.

[Weber, W. et al. 2005]. Ambient Intelligence, Springer Verlag, Berlin, 2005.

[Weiser, M. 1991]. The computer for the twenty-first century. Scientific Am 265(3):91-104, 1991.

[Aarts, E. Manzano, 2003]. The new everyday: Views of Ambient Intelligence. 010 Publishers (2003) Rotterdam, 2003.

[Nieuwoudt, C. and Botha, EC. 2002]. Cross-language use of acoustic information for automatic speech recognition. Speech communication 38:101-113, 2002.

[Rebman, CMJ. et al. 2002]. Speech Recognition in the Human-computer Interface. Information and Management 2011:1-11, 2002.

[Reynolds, F. et al. 2006]. The ubiquitous Web, UPnP and Smart Homes. Cambridge, UK: a Pervasive Computing Group Nokia Research Center, Cambridge, UK. 2006.

[Jean Baptiste, 2007]. "Nano-informatique et intelligence ambiente", Jean Baptiste Waldner, Hermes Science Publishing, 2007.

[Ubiquitous computing: Towards understanding European Strengths and Weaknesses, 2000]. Draft final report, prepared by PREST, CMI, INRIA/OST, Fondazione Rosselli, ITA, VTT Electronic, December 2000.

[Friedewald, M. et al. 2005]. Perspectives of ambient intelligence in the home environment. Telematics Informatics, 22, Elsevier, 221-238, 2005.

[Encarnacao, J.L. & Kriste, T. 2005]. Ambient intelligence: Towards smart appliance ensembles. M. Hemmje et al. Eds., Lecture Notes in Computer Science, vol. 3379, Sprinter, Berlin Germany, 261-270, 2005.

[Haux, R. 2006]. Individualization, globalisation and health-about sustainable information technologies and the aim of medical informatics. Int. J. Medical Informatics 75, Elsevier, 795-808, 2006.

[Garate, A. et al. 2005]. GENIO: An ambient intelligence application in home automation and entertainment environment. In Proceedings of the Joint sOc-EUSAI Conference, 241-245, 2005.

[Cook, D.J. et al. 2006]. A multi-agent approach to controlling a smart environment. In Designing Smart, The Role of Artificial Intelligence, J. C Augusto and C.D. Nugent, Eds., Lecture Notes in Artificial Intelligence, vol. 4008, Springer, Berlin Germany, 165-206, 2006.

[Riva, G. 2003]. Ambient intelligence in health care. Cyber Psych. Behav. 6, 3, Mary Ann Liebert, Inc. Publishers, 295-300, 2003.

[Gouaux, F. et al. 2002]. Ambient intelligence and pervasive systems for monitoring of citizens at cardiac risk: New solutions from the EPI-MEDICS project. Comput. Cardiol. 29, 289-292, 2002.

[http://epi-medics.insa-lyon.fr/statico/epimedica.htm], 2014.

[Muñoz, M.A. et al. 2003]. Context aware mobile communication in hospitals. IEEE Comput. 36, 38-46, 2003.

[Favela, J. et al.2004]. Integrating context-aware public displays into a mobile hospital information systems. IEEE Trans. Inf. Technol. Biomed. 8, 3, 279-286, 2004.

[Rodríguez, M. et al. 2004]. Location-aware access to hospital information and services. IEEE Trans. Inform. Technol. Biomed. 8, 4, 448-455.

[Rodríguez, M. et al, 2005] Agent-based ambient intelligence for healthcare. AI Comm. 18, 3, 201-216, 2004.

[Kanstrup, A.M. et al. 2008]. PDC'08 Proceedings of the 10th Anniversary Conference on Participatory Design. Design for More: an Ambient Perspective on Diabetes, 2008-Bloomington, USA.

[Silva, J.M. et al. 2009]. Proceedings of the 1st ACM SIGMM International Workshop on Media Studies and Implementations that help improving access to disabled users: UbiMeds: A mobile application to improve accessibility and support medication adherence, 2009-Beijing, China.

[Heinzelman, W. et al. 2004]. Middleware to support sensor network applications. IEEE Network, 18:2004, 2004.

[Jung, D. et al. 2005]. A mobile alerting system for the support of patients with chronic conditions. In First European Conference on Mobile Government (EUROmGOV), Brighton, UK, pages 264-274, 2005.

[Corchado, J.M. et al. 2008]. GerAmI: improving healthcare delivery in geriatric residences. J. IEEE Intelligent Systems (Special Issue on Ambient Intelligence), 3, 2, 19-25, 2008.

[Doyle, J. et al. 2010]. BCS'10 Proceedings of the 24th BCS Interaction Specialist Group Conference. Designing a touch screen communication device to support social interaction amongst older adults. 2010-Dundee, UK.

[Niemela, M. et al. 2007]. Supporting independent living of the elderly with mobile-centric ambient intelligence: user evaluation of three scenarios, B. Schiele et al. Eds., Lecture Notes in Computer science, vol. 4794, Springer-Verlag Berlin, 91-107, 2007.

[Carmichael, A. et al. 2010]. BCS'10 Proceedings of the 24th BCS Interaction Specialist Group Conference: Investigating a DTV-based physical activity application to facilitate wellbeing in older adults. 2010-Dundee, UK.

[Hanson, Mark A. et al. 2011]. Proceedings of the 2nd Conference on wireless Health'11, San Diego, USA. In Home assessment and Management of Health and Wellness with BeClose TM Ambient, Artificial Intelligence, October 2011, San Diego, USA.

[A.J. Jara, et al. 2011]. An Internet of things-based personal device for diabetes therapy management in AAL. April 2011 Personal and Ubiquitous Computing, Vol. 15 Issue 4, 2011.

[J. Sidén, et al. 2011]. Home care with NFC Sensors and A Smart Phone. October 2011 Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communications Technologies ISABEL'11, Barcelona, Spain, 2011.

[Marcela D. Rodríguez, et al. 2011]. Design Dimensions of Ambient Information Systems to Facilitate the Development of AAL Environments. PETRA'11 Proceedings of the 4th International Conference on PErvasive Technologies Related to Assistive Environments. Crete, Greece, May 2011.

[Holzinger, A. et al, 2005]. Lifelong-learning support by mlearnig: Example scenarios, eLearn, 11 (2005), 2, 2005.

[Rogers, Y. et al. 2005]. Ubi-learning integrates indoor and outdoor experiences. Communications of the ACM, 48, 1 (2005), 55-59, 2005.

[Costabile, María F. et al. 2008]. Explore! Possibilities and Challenges of Mobile Learning, CHI'08 Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing. CHI 2008 Proceedings-Learning Support, April 2008 Florence, Italy, 2008.

[Ciancio, E. et. al. 2000]. Come explorare l'area archeologica di Monte Sannace, Laterza, Bari, Italy 2000.

[Aroyo, L & Kommers, P. 2001]. Special issue preface, Intelligent Agents for Educational Computer-aided Systems. Interactive Learning Research, 10 (3/4), 235-242, 2001.

[Johnson W.L., Rickel J.W. & Lester J.C. 2000]. Learning Environments, International Journal of Artificial Intelligence in Education, 11 (2000), (47-78), 2000.

[Klopfer, E. et al. 2005]. Mystery at the museum: a collaborative game for museum education. Proc. CSCL 2005, ACM Press (2005), 316-320, 2005.

[S. Sun, M.S. Joy, 2005]. Proceedings of the 23rd IASTED International Multi-Conference Artificial Intelligence and Applications. February 2005, Innsbruck, Austria.

[R. Wakkary, et al. 2009]. Kurio: A Museum Guide for Families. TEI'09 Proceedings of the 3rd International Conference on Tangible and Embedded Interaction. February 2009.

[C.X. Navarro, et al. 2015]. Framework para Evaluar Sistemas M-learning: Un enfoque tecnológico y Pedagógico, VAEP-RITA Vol. 3, Núm. 1, Mar.2015 ISSN 2255-5706 (IEEE-ES), 2015.

[Da Silva, F.S. and Vasconcelos, W.W. 2007]. Managing responsive environments with software agents. J. Appl. Artif. Intell. 21, 4, 469-488, 2007.

[Masthoff, J. et al. 2007]. Agent-based group modelling for ambient intelligence. In Proceedings of the AISB Symposium on Affective Smart Environments. P. Oliver and C. Kray, Eds. 90-96, 2007.

[A. Geven, et al. 2007]. HCI'07 Proceedings of the 9th International Conference on Human Computer Interaction with Mobile Devices and Services: Experiencing Real-World Interaction: Results from a NFC User Experience Field Trial, Singapore, 2007.

[Kopacsi, S. et al. 2007]. Ambient intelligence as enabling technology for modern business paradigms. Robotics Comput.-Integrat. Manufactur. 23, 247-256, 2007.

[Werner Weber, 2003]. Ambient Intelligence-Industrial Research on a Visionary Concept. In Proceedings of the 2003 International Symposium on Low Power Electronics and Design, ISLPED'03, 247-251. August, 2003, Seoul, Korea.

[Keegan, S. et al. 2008]. Easishop: ambient intelligence assists everyday shopping. J. Inform. Sci. 178, 3, 588-611, 2008.

[P. DeVries, 2008]. The state of RFID for effective baggage tracking in the airline industry. International Journal of Mobile Communications 2008. 6(2):151-164, 2008.

[Bosse, T. et al. 2008]. A component-based ambient agent model for assessment of driving behavior. In Proceedings of the 5th International Conference on Ubiquitous Intelligence and Computing (UIC). F. E. Sandnes, Y. Zhang, C. Rong, L. T. Yang, J. Ma, Eds., Lecture Notes in Computer Science, vol. 5061, Crpinger, Berlin, 229-243, 2008.

[J. Reason & R. Crepaldi, 2009]. Ambient Intelligence for freight railroads. IBM Journal of Research and Development, 53 (3), 2009.

[Tomás Sánchez López et al. 2011]. Adding sense to the Internet of Things. Personal and Ubiquitous Computing, Vol. 16, Issue 3, pp. 291-308. June, 2012.

[Karacapilidis, N. and Papadias, D. 2001]. Computer supported argumentation and collaborative decision making: The Hermes system. Infor. Syst.26, 4, 259-277, 2001.

[Prakken, H. and Gordon, T.F. 1999]. Rules of order for electronic group decision making- a formalization methodology. In Proceedings of the VIM Spring and Winter Workshops on Collaboration between Human and Artificial Societies. Lecture Notes in Artificial Inteligence, vo. 1624, Springer Verlag, Berlin, 246-263, 1999.

[Gonzalez, G. et al. 2004a]. Managing emotions in Smart user models for recommender systems. In Proceedings of 6th International Conference on Enterprise Information Systems (ICEIS). 5, 187-194, 2004.

[Gonzalez, G. et al. 2004b]. Smart user models for tourism: A holistic approach for personalized tourism services. Inform. Technol. Tourism J.: Applicat. Methodol. Tecniques, 6, 4, Cognizant Communication Corporation, 2004.

[Gonzalez, G. et al. 2005]. Smart user models for ambient recommender systems. In Ambient Intelligence and (Everyday) Life, Y. Cai, Y. and J. Abascal Eds., University of Basque Country, San Sebastian, Spain, 113-122, 2005.

[Gonzalez, G. et al. 2006]. Towards ambient recommender systems: Results of new cross-disciplinary trends. In proceedings of ECAI Workshop on Recommender Systems, 2006.

[Rumetshofer, H. et al. 2003]. Individual information presentation based on cognitive styles for tourism information systems. In Proceedings of the International Conference on Information and Communication Technologies in Tourism. A. J. Frew, M. Hitz, and P. O'Connor, Eds., Springer Verlag, Berlin, 440-449, 2003.

[Manes, G. 2003]. The Tetherless Tourist: Ambient Intelligence in Travel & Tourism. Information Technology & Tourism 5, 211-220, 2003.

[Staab, S. et. al. 2002]. Intelligent Systems for Tourism: Trends & Controversies. IEEE Intelligent Systems 6, 53-66, 2002.

[Oyster mobile wallet, Londor underground, 2008]. http://www.tflgov.uk/

[Monaco City Museum, 2009]. http://2009.wima-fc.com/content/Deploying-NFC-technology-in-the-Nouveau-Musee-National-de-Mocaco, 2009.

[Liikka, J. et al. 2008]. Mobile Guide for the City Traveller. In: 4th International Conference on Intelligent Environments, pp. 1-7, July 2008, Seattle, USA.

[Bojen Nielsen, L.MA. 2004]. ICEC'04. Post Disney experience paradigm? Some implications for the development of content to mobile tourist services. In Proceedings of the 6th International Conference on Electronic Commerce. March, 2004-Delft, The Netherlands.

[Penserini, L. et al. 2005]. Using Tropos to model agent based architectures for adaptive systems: A case study in ambient intelligence. In Proceedings of the IEEE International Conference on Software-Science, Technology and Engineering (SwSTE). IEEE Press, 2005.

[Constantini, S. et al. 2008]. DALICA: Agent-based ambient intelligence for cultural heritages scenarios. IEEE Intell. Syst. (Special Issue on Ambient Intelligence), 23, 2, 34-41, 2008.

[Petersen, S. and Kofod-Petersen, A. 2006]. The non-accidental tourist: Using ambient intelligence for enhancing tourist experiences. In Network-Centric Collaboration and Supporting Frameworks, L. Camarinha-Matos, H. Afsarmanesh, and M. Ollus, Eds., International Federation for Information Processing (IFIP). Vol. 224, 619-626. 2006.

[Borrejo-Jaraba, F. et al. 2010]. Proceedings of the 23rd International Conference on Industrial Engineering and other Applications of Applied Intelligent Systems. Volume Part III, pp. 229-238. IEA/AIE'10. NFC Solution for the Development of Smart Scenarios Supporting Tourism Applications and Surfing in Urban Environments, 2010-Córdoba, Spain.

[El internet de las cosas. Monográfico de la revista BIT, nº 187, 2011]. Editado por el COIT, Colegio Oficial de Ingenieros de Telecomunicación y la AEIT, Asociación Española de Ingenieros de Telecomunicación, 2011.

[Min Chen, et al. 2011]. Body Area Networks: A Survey. Mobile Networks and Applications, Vol. 16, Issue 2, 171-193. April 2011.

[A. Weder, et al. 2011]. A Mobile System for Precise Wireless Pulse Transit Time (PTT) Monitoring. Mobile Health'11 Proceedings of the First ACM Mobil Hoc Workshop on Pervasive Wireless Healthcare, Paris, France, May 2011.

[J. Espina, et al. 2008]. Wearable body sensor network towards continuous cu-less blood pressure monitoring. ISSS MDBS 2008, 5th International Summer School and Symposium on Medical Devices and Biosensors, pp. 28-32, 2008.

[Veselin Ganev, et al. 2011]. The Smart Condo: Integrating Sensor Networks and Virtual Worlds. SESENA'11 Proceedings of the 2nd Workshop on Software Engineering for Sensor Network Applications, Waikiki, Honolulu, HI, USA, 2011.

[J.S. Bermúdez et al. 2011]. Communications system in a Smart accelerometric sensor for monitoring of physical risk events. ISABEL'11 Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies. Barcelona, Spain. October 2011.

[Jeffrey W. Lockhart, et al. 2011]. Design Considerations for the WISD; Smart Phone-based Sensor Mining Architecture. SensorKDD'11 Proceedings of the 5th International Workshop on Knowledge Discovery from Sensor Data. San Diego, CA. USA. August 2011.

[I. Akyildiz, et al. 2002]. A survey on sensor networks, IEEE Communications Magazine, Volume: 40, Issue: 8, 2002.

[M. Gaynor, et al. 2004]. Integrating wireless sensor networks with the grid, IEEE Internet Computing, 2004.

[E. Gavin, et al. 2009]. Applying and extending sensor web enablement to a telecare sensor network architecture, In COMSWARE'09: Proceedings of the Fourth International ICST Conference on COMmunications System softWAre and middlewaRE, 2009.

[S. Patel et al. 2010]. Home Monitoring of Patients with Parkinson's Disease via Wearable Technology and a Web-based application. 32nd Conference of the IEEE EMBS, 2010.

[B. Son, et al. 2006]. A design and implementation of forest-fires surveillance system based on wireless sensor networks for South Korea mountains. International Journal of Computer Science and Network Security, 2006.

[N. Markovic, et al. 2009]. Sensor Web for River Water Pollution Monitoring and Alert System, 12th AGILE International Conference on Geographic Information Science Advances in GIScience, Hannover, Germany, 2009.

[E. Miluzzo, et al. 2008]. Sensing meets mobile social networks: The design, implementation and evaluation of the cenceme application. Proceedings of SenSys, 2008.

[A. Beach, et al. 2008]. Whozthat? Evolving an ecosystem form context-aware mobile social networks, IEEE Network, 2008.

[Laukkanen, M. 2007]. Towards Operating Identity-based NFC Services. IEEE International Conference on Pervasive Services, 2007.

[Geven, A. et al. 2007]. Experiencing real-world interaction: Results from a NFC user Experience field trial. 9th International Conference on Human Computer interaction with Mobile Devices and Services, September, 2007.

[Lahtela, A. et al. 2008]. RFID and NFC in healthcare: Safety of hospitals medication care. Second International Conference on Pervasive Computing Technologies for Healthcare, PervasiveHealth 2008, pp. 241-244. February 2008.

[Bravo, J. et al. 2008]. Identification technologies to support Alzheimer contexts. 1st International Conference on Pervasive Technologies Related To Assistive Environments, PETRA'08, vol. 282. July, 2008.

[B. Ullmer and H. Ishii, 2001]. Emerging frameworks for tangible user interfaces, in: J.M. Carrol (ed.), Human Computer Interaction in the New Millenium, Addison Wesley, Reading, MA, USA, pp. 579-601, 2001.

[Maybury, M. 1999]. Intelligent user interfaces: an introduction. In Proceedings of the 4th International Conference on Intelligent User Interfaces, IUI'99. ACM Press, New York, USA, 3-4, 1999.

[Russel, et al. 1995]. Artificial Intelligence: A Modern Approach. Englewood Cliffs, NJ: Prentice-Hall, 1995.

[P. Maes, 1995]. Agents than Reduce Work & Information Overloada, Baecker, Grudin, Buxton and Greenberg, Readings in HCI: Human-Computer Interaction Toward the Year 2000, pp. 811-822, Morgan and Kaugmann Publishers, San Francisco, USA, 1995.

[Franklin S, et al. 1996]. Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents. Proceedings of the Third International Workshop on Agent Theories. Architectures, and Languages. Springer-Verlag, 1996.

[Foner, L.N. 1993]. What's an agent, anyway? A sociological case study. Agents Memo 93-01, Agents Group, MIT Media Lab. 1993.

[Shoham, Y. 1993]. Agent Oriented Programming. Artificial Intelligence, Vol. 60, nº 1, pp. 51-92, 1993.

[N. R. Jennings and M. Wooldridge, 1998]. Applications of Intelligent Agents. Agent Technology Foundations, Applications, Applications and Markets, Springer-Verlag, 1998.

[J.M. Corchado and J.M. Molina, 2001]. Introducción a la Teoría de Agentes y Sistemas Multiagente. Universidad de Salamanca, España 2001.

[Wooldridge & Jennings, 1995]. Intelligent Agents: Theory and Practice. The Knowledge Engineering Review, vol. 10(2) pp. 115.152, 1995.

[Maes, P. 1989]. Situated Agents Can Have Goals. Designing Autonomous agents: Theory and Practice From Biology to Engineering and Back, pp. 49-71, Maes, Pattie, (Ed), 1989.

[Jennings, N.R. 1993]. Specification and implementation of a belief-desire-joint-intention architecture for collaborative problem solving. Int, J. Intell. Coop. Inf. Syst., 289-318, 1993.

[Rao, A.S., et al. 1995]. BDI Agents from Theory to Practice. Proceedings of the First International Conference on Multi-Agents Systems (ICMAS-95), San Francisco, June 1995.

[Brooks, R.A. 1991]. Intelligence without Representation. Artificial Intelligence, 47, 139-159, 1991.

[Huhns, M.N., et al. 1998]. Multiagent systems in information-rich environments. In: Klusch M., Weib G. (eds). Cooperative Information Agents II Learning, Mobility and Electronic Commerce for Information Discovery on the Internet. CIA 1998. Lecture Notes in Computer Science, vol. 1435. Springer, Berlin, Heidelberg, 1998.

[Corchado, J.M. et al. 2008]. A multi-agent architecture for distributed services and applications. Computational Intelligence 24 (2), 77-107, 2008.

[K. Z. Haigh, et al. 2002]. An open agent architecture for assisting elder independence. *AAMAS'02,* July 15-19, 2002, Bologna, Italy.

[A. Muñoz, et al. 2001]. Design and Evaluation of an AAL system based on an augmentative multi-agent system. Personal and Ubiquitous Computing, Vol. 15 Issue 4, 377-387. April, 2001.

[Bombara et al. 2003]. A multi-agent System to assist museum visitors. In Proceedings of the Workshop on Objects and Agents (WOA2003), Cagliari, Italy, 2003, pp. 175-178.

[Moreno et al. 2003]. Using JADE-LEAP to implement agents in mobile devices; TILAB "EXP in search of innovation", Italy, 2003.

[Susperregi et al. 2004]. Una arquitectura multiagente para un Laboratorio de Inteligencia Ambiental en Fabricación. Desarrollo de Sistemas Multiagente DESMA-2004, en colaboración con IX Jornadas de Ingeniería del Software y Bases de Datos. Noviembre, 9 Málaga, Spain, 2004.

[Corchado et al. 2008]. Intelligent environment for monitoring Alzheimer patients, agent technology for health care. Decision Support System. Elsevier Science Publishers B.V. Amsterdam (The Netherlands), 2008, vol. 44. Issues 2, pp. 382-396.

[Spanoudakis and Moraitis, 2006]. Agent Based Architecture in an Ambient Intelligence Context. Proc. 4th European Workshop Multi-Agent Systems (EUMAS06), 2006, Lisbon, Portugal, pp. 163-174.

[Fraile, J.A. et al. 2008]. AMADE: Developing a Multi-Agent Architecture for Home Care Environments. In 7th Ibero-American Workshop in Multi-Agent Systems. Lisbon, Portugal, 2008.

[W.L. Johnson, et al. 2000]. Animated Pedagogical Agents: Face-to-Face Interaction in Interactive Learning Environments. International Journal of Artificial Intelligence in Education, 11, 2000.

[Mbala and A.G.N. Anyouzoa, 2005]. A multi-agent system to support users in online distance learning. In Agent-based Systems for Human Learning, AAMAS Workshop, 2005.

[K. Sehaba and P. Estraillier, 2005]. A multi-agent system for rehabilitation of children with autism. In Agent-based Systems for Human Learning, AAMAS Workshop, 2005.

[J. Pavón, et al. 2007]. Development of intelligent multisensory surveillance systems with agents, Robotics and Autonomous Systems 55 (12), 2007, pp. 892–903.

[H. Vagts, et al. 2011]. In Proceedings of the 4th International Conference on Pervasive Technologies Related to Assistive Environments, PETRA'11, Crete, Greece 2011.

[Bryce, C. et al. 2007]. Ubiquitous privacy protection. 2007 Presented at: First IEEE International Workshop on Privacy in Ubiquitous Systems; August 2007, Salzburg, Austria.

[Westin, A.F. 2003]. Social and political dimensions of privacy. J Social Issues 2003 Jun; 59(2): 431-453 (doi: 10.1111/1540-4560.00072), 2003.

[Sweeney, L. 2001]. Computational disclosure control: A primer on data Privacy protection, Ph. D Thesis, MIT, 2001.

[De Hert, P. et al. 2009]. Pers Ubiquit Comput (2009) 13:435-444. Legal safeguards for privacy and data protection in ambient intelligence. Springer-Verlag London Limited 2008.

[Altman, I. 1975]. The Environment and Social Behavior: Privacy, Personal space, Territory and Crowding. Brooks/Cole Publishing Company, CA, 1975.

[Langheinrich, M. 2002]. A privacy awareness system for ubiquitous computing environments. In UbiComp'02. Srpinger, 2002.

[Hong, J.I. et al. 2004a]. An architecture for privacy-sensitive ubiquitous computing. In MobySys'0. ACM, 2004.

[Krumm, J. 2009]. A survey of computational location privacy. Pers. and Ubiquitous Comp., 13 (6), 2009.

[Sheikh, K. et al. 2008]. Quality-of-Context and its use for Protecting Privacy in Context Aware Systems. Journal of Software, 3(3): 83-93, 2008.

[Hesselman, C. et al. 2008]. Controlled Disclosure of Context Information across Ubiquitous Computing Domains. In Intl. Conf. Sensor Networks, Ubiq., and Trustworthy Comp. (SUTC'08). IEEE, 2008.

[Wright, D. et al. 2008]. SWAMI: Dark Scenarios. Safewards in a world of ambient intelligence, Springer Press, Dordrecht, p291, 2008.

[Friedewald, M. et al. 2005]. Perspectives of ambient intelligence in the home environment. Telematics Informatics, 22, Elsevier, 221-238, 2005.

[Bohn, J. et al. 2004] Living in a world of smart everyday objects-Social, economic, and ethical implications. Human Ecol. Risk Assess., 10, 5.2004.

[Rouvroy, A. 2008]. Privacy, data protection, and the unprecedented challenges of ambient intelligence. Studies Ethics, Law, Technol. 2, 1, Article 3.2008.

[Reiter, M. et al. 1999]. Crowds: Anonymity for web transactions. Communications of the ACM, vol. 42, nº 3, pp. 32-48, 1999.

[Serjantove, A. et al. 2002]. Towards an information theoretic metric for anonymity. Proceedings of Workshop on Privacy Enhancing Technologies (PET'02), LNCS 2482. Springer-Verlag, 2002.

[Díaz, C. et al. 2002]. Towards measuring anonymity. In: Privacy Enhancing Technologies: Second International Workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002: revised papers. New York: Springer-Verlag: 54-68, 2003.

[Agrawal, D. et al. 2001]. On the design and quantification of privacy preserving data mining algorithms. Symposium on Principles of Database Systems (PODS'01), pp. 247-255, Santa Barbara, May 2001.

[Hong, J.I. et al. 2004b]. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. DIS'04 Proceedings of the 5th Conference on Designing Interactive Systems. 91-100, 2004.

[Friedewald, M. et al. 2007]. Privacy, identity and security in ambient intelligence: a scenario analysis. Telematics Informatics 2007 Feb; 24 (1):15-29.

[Adams, A. et al. 2001]. Privacy in multimedia communications: protection users, not just data. 2001 Presented at: Joint Proceedings of Human-Computer Interaction/Interaction d' Homme-Machine (IMH-HCI 01); 2001; Lille, France pp: 49-64.

[Kapadia, A. et al. 2007]. Virtual walls: protecting digital privacy in pervasive environments. In LaMarca A, Langheinrich M. Truong KN, editors. Pervasive Computing: 5th International Conference, PERVASIVE 2007, Toronto, Canada, May 13-16, 2007. Proceedings (Lecture Notes in Computer Science/Information… Applications, incl. Internet/Web, and HCI): Verlag Berlin, Heidelberg: Springer-Verlag; 2007: 162-179.

[Lederer, S. et al. 2002]. Report N, UCB/CSD-2-1288. Berkeley, CA, USA: University of California; 2002 Jun. A conceptual model and metaphor of everyday privacy in ubiquitous computing environments.

[Garimella Rama Murthy, 2006]. Fundamental Limits on a Model of Privacy-Trust Tradeoff: Information Theoretic Approach. International Journal of Network Security, Vol. 3, Nº 3, pp. 225-229. November 2006.

[Abdul-Rahman, A. et al. 2000]. Supporting trust in virtual communities, 2000. Proceedings of the 33rd Hawaii. International Conference on System Sciences; Jan 4-7, 2000; IEEE Computer Society, Washington, DC, USA.

[Billhardt H. et al. 2007]. Trust-based service provider selection in open environments. New York, NY, USA: ACM; 2007 Presented at: Proceeding of the ACM Symposium on Applied Computing; 2007; Seoul, Korea p. 1375-1380.

[McKnight DH, Et al. 2002]. Developing and validating trust measures for e-commerce: an integrative typology. Inform Sys Res 2002 Sep. 13(3):334-359.

[Liu Z, Yau et al. 2008]. A flexible trust model for distributed service infrastructure. USA: IEEE; 2008 Presented at: Proceeding of the 11th Symposium on Object Oriented Real-Time Distributed Computing (ISORC); May 7-5, 2008; Orlando, USA p. 108-115.

[Lu Y. et al. 2006]. Trust-based privacy preservation for peer-to-peer data sharing. IEEE Trans SystMan Cybern A 2006 May;36(3):498-502.

[Almenarez F, et al. 2004]. Managing ad-hock trust relationships in pervasive computing environments. 2004 Presented at: Proceedings of the Workshop on Security and Privacy in Pervasive Computing SPPC; 2004; Vienna, Austria.

[Ruotsalainen, PS. et al. 2012]. A conceptual framework and principles for trusted pervasive health. J. Med Internet Res 2012, Apr; 14(2):e52. (doi:10.2196/jmir.1972).

[Clarke, R. 1997]. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. http://www.rogerclarke.com/DV/Intro.html.1997.

[K. Fullam, et al. 2005]. A specification of the agent reputation and trust (art) testbed: experimentation and competition for trust in agent societies, in: The Fourth International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS-2005, pp. 512-518, 2005.

[C. Dellarocas, 2003]. The digitization of Word of mouth: promise and challenges of online feedback mechanisms, Manag. Sci. 49 (2003). 1407-1424.

[J. Sabater-Mir, C. Sierra, 2005]. Review on computational trust and reputation models, Artif. Intell. Rev. 24 (2005), 33-60.

[B. Yu, M.P. Singh, 2002]. An evidential model of distributed reputation management, in: Proceedings of First International Joint Conference on Autonomous Agents and Multiagent Systems, ACM Press, 2002, pp. 294-301.

[B-Esfandiari, S-Chandrasekaran, 2001]. On how agents make friends: mechanisms for trust acquisition, in: Proceedings of the Fourth Workshop on Deception, Fraud in Trust in Agent Societies, 2001, pp. 27-34.

[Regulation EU, 2016/679]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119 (4 May 2016) 1-88.

[J, Moya and J. Carbo, 2012]. Distributing art agents with jade, in: 10th European Workshop on Multi-Agent Systems, EUMAS, 2012.

[J. Carbo and J.M. Molina, 2009]. A jade-based art-inspired ontology and protocols for handing trust and reputation, in: Ninth International Conference on Intelligent Systems Design and Applications, ISDA, 2009, pp. 300-305.

[F.L. Bellifemine, et al. 2007]. Developing Multi-Agent Systems with JADE, Wiley, 2007.

[Competition of ART testbed, 2007]. http://megatron.iiia.csic.es/art-testbed/competiiton_results 2007.htm.

[UNO]. @in collection uno2008. Title: Strategies for Exploiting Trust Models in Competitive Multi-Agent Systems. Author: Munoz, Víctor and Murillo, Javier and Lopez, Beatriz and Busquets, Dídac. Book title Multiagent System Technologies, Lecture Notes in Computer Science, Editor Braubach, Lars and van der Hoek, Wiebe and Petta, Paolo and Pokahr, Alexander, Springer Berlin / Heidelber, pages 79-90, volume 5774, 2009.

[ZeCarioca]..http://www.researchgate.net/publication/228731165_Ze_Carioca_LES-Finalista_da_Competicao_Agent_Reputation_Trust_ART_Testbed, 2010.

[AFRASArt]. @article softcomputing. Title: An extension of a fuzzy reputation agent trust model (AFRAS) in the ART testbed. Author: Carbo,, Author Javier and Molina,, Jose M., Journal Sofcomputing, volume 14, number 8, pages 821-831, 2010.

[IAM]. @in proceedings iam. Title: The ART of iam: The winning strategy for the 2006 competition. Author W.T. LukeTeacy and T.D. Huynh and R.K. Dash and N.R. Jennings and J. Patel and M. Luck. Book title: Procs. of Trust in Agent Societies WS Procs., AAMAS 2007.

[WEKA, v.3.6.1.]. http://www.cs.waikato.ac.nz/ml/weka/downloading.html.

[M. Esteva, et al. 2002]. Islander: an electronic institutions editor, in: The First International Joint Conference on Autonomous Agents & Mutiagent Systems, AAMAS, ACM, 2002, pp. 1045-1052.